Cybersecurity Is Too Important To Be Left To The Specialists

Anonymous

Abstract—**There are numerous facets to cybersecurity education, from theory to practice, hardware and software, to social and technical (as well as other important dimensions). A multitude of national and international model curricula and recommendations - from national academies, learned societies and even governments – have been presented and discussed in recent years, with varying levels of impact on policy and practice. In this paper we attempt to address the key questions "what should the generalist computer scientist/engineer know" and "how well is that being taught". (Cyber)security – if thought about at all – has historically been left to specialists, frequently viewed as a masters-level discipline; or left for development in professional practice, sometimes called "information assurance" in the UK and Europe, which worked, even if not well, in a sequential process model.**

For example, in the world of software and systems development, we have seen the disruption of Agile (invented c.2001) and DevOps (invented c.2009), but not necessarily through the lens of security; however, more recently there has been a recognition of the need for change, exemplified by the emergence of "DevSecOps". If security is not to be left to the experts, then the generalist must know about it. Thus, in the context of widespread international computer science/engineering curriculum reform - both in compulsory, as well as post-compulsory education - what does this trend mean more generally for institutions and educators, and how do we teach it?

In this paper, we frame a key social, cultural and economic global challenge of cybersecurity in computing and engineering education by analysing the UK's national security, economic, and skills policy context, shaping the practical considerations for education professionals from schools through to universities (and into industry and professional practice). Through this analysis of UK educational policy and practice, we make a number of recommendations for future cybersecurity educational initiatives and interventions, including a number of innovative practical suggestions for educators and curriculum designers, with a view for potential adoption and adaption in other jurisdictions internationally.

Index Terms—**Cybersecurity, accreditation, curricula, computer science education, UK**

I. Introduction

Cybersecurity has increasingly been in the news over recent years, generally prompted by spectacular breaches of one kind or another, such as [1]. It needs attention across the spectrum:

> change the culture in your organisation around cyber security; to try to do for cyber what has been done so successfully for health and safety, for example, over the last ten years — to get everybody to take it seriously; to take the risk management process seriously and drive that down through the organisation. [2][1]

With this significant economic and societal focus on cybersecurity, there are calls for formal education – school-level as well as post-compulsory – to respond to this situation, which it does both at the individual level and via recommended curricula [3] and professional accreditation requirements [4]; this is alongside a wider focus on computer science education reform, especially across the UK [5], [6], [7], [8], [9], [10], [11], [12], [13]. There has been a recent international working group [14], but this has yet to report. We note that part of its third aim is to "catalog existing [. . .] knowledge materials", but there is no mention of any quality control over these (see section III-B).

Nevertheless, it is one thing to write national curricula, specifications and requirements, and another thing to deliver appropriate and relevant education and skills; furthermore, one could reasonably ask how well this is done in practice.

A. CyberSecurity: for all or for specialists?

In one sense, this title is a false dichotomy: there is a serious need for cybersecurity specialists (estimates vary, but are always large: [15] has only anecdotal evidence), but also all in IT need to know *some* cybersecurity, as the recent fashion for talking about DevSecOps rather than just DevOps exemplifies.

This is not a brand-new concern: see [16] for concerns over five years ago, but it is a growing one. On the one hand, GDPR has increased the corporate penalties for failure, and therefore the demand for various forms of cybersecurity specialists, both explicitly by requiring Data Protection Officers[2] and implicitly by causing boards to invest more in cybersecurity. On the other hard, the growing publicity given to these, and the growing use of electronic payment, has also led to greater demand for staff in this area.

In particular the expectation of "Privacy by Design" and and by "Privacy by Default" has significant implications for all software development with a European context that processes personal data. Whilst both "Privacy by Design" and "Privacy by Default" have been expected good practices for a number of years, these expectations now have a legal dimension, at least in Europe.

However, "Privacy by Design" is no good without "Security by Implementation", and many security weaknesses

[1] Former Director of GCHQ: British equivalent of NSA.

[2] [17] places quite strong requirements on these: "expertise in national and European data protection laws and practices and an in-depth understanding of the GDPR", as well as "principles of data processing", "data protection by design and by default" and "security of processing". It is hard to envisage one person possessing all these attributes, and indeed "DPO as a service" is being promoted [18].

are implementation weaknesses. A number of studies have documented the challenges of aligning security methods in Agile Practices [19]. This further emphasizes the need for mainstream software developers and by extension Computer Science graduates to be versed in relevant security practices.

The Payments Industry [20, 6.6] insists on either independent code reviews by security specialists or a Web Application Firewall: essentially saying that the normal development process even after developers are trained in secure coding practices [20, 6.5] cannot be trusted to deliver secure code. This would seem to be particularly the case with "agile" processes [21].

Specialist curricula abound: a recent one is [22]. However, given the shortage of specialists, in practice a good generalist with some cybersecurity expertise can often get a "specialist" job.

B. Research Questions

There are various levels of specialism at which cybersecurity education can be addressed.

1) The person in the street — this is important, but there are many initiatives in this area, which are, rightly, largely separated from computing education.
2) The general CS graduate.
3) The general CS masters graduate.
4) The specialist CS graduate.
5) The specialist CS masters graduate.

The focus of this paper is on 2–3: the general CS graduate.

RQ1 What should be taught to the generalist, and how?
RQ2 Should this be taught stand-alone or integrated?
RQ3 How might accreditation regard cybersecurity Education, or help with it?

[3, p. 97] takes a distinct view on RQ2:

> The Information Assurance and Security KA is unique among the set of KAs presented here given the manner in which the topics are pervasive throughout other Knowledge Areas.

It proposes 9 "core" hours and 63.5 distributed across the other Knowledge Areas.

Nevertheless, the situation on the ground is different: [23], describing the USA, writes as follows

> Universities suffer shortcomings, as well. Roughly 85 of them offer undergraduate and/or graduate degrees in cybersecurity. There is a big catch, however. Far more diversified computer science programs, which attract substantially more students, don't mandate even one cybersecurity course.

But [24, Table 1] shows that the UK situation is distinctly different: he quotes that 61% of UK courses offer mandatory cybersecurity content, and his research was based on web scraping, it represents a lower bound.

It is at least plausible to attribute this difference to differences in the accreditation regimes.

UK BCS has had a requirement to include information security in the curriculum since 2010, and has expected coverage of an agreed cybersecurity syllabus since 2015 (Table I), with the result that all accredited universities should be compliant by 2020 (because of the five-year cycle). More precisely since 2010, 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" [4, p. 30] since 2010 with an enhanced cybersecurity related definition of what this entails since 2015 [4, p. 17–18].

US ACM has equally had cybersecurity ("Information Assurance and Security" — IAS) in the curriculum since 2013 [3], but it is not the accrediting body. ABET is, and is requiring IAS with effect from the 2019-20 cycle (self study reports due 1 July 2019): more precisely [25, 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 (because of the six-year cycle).

II. Policy Context

There has been substantial CS/digital curriculum reform across the UK [5], [6], [8], [7], [9] — but what has happened to the focus on cybersecurity? The Institute of Coding [26], designed to improve digital skills for UK graduates, does indeed mention cybersecurity, but merely as a sub-item in one work package (1.2a).

UK national economic skills priority e.g. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 (especially [15] and https://www.ncsc.gov.uk/blog/skills-and-training and https://www.cybersecuritychallenge.org.uk/).

There is large-scale media attention on the "cybersecurity skills gap" e.g. https://www.contracts.mod.uk/do-features-and-articles/digital-skills-shortage-threatens-uk-cyber-security/ and https://www.itpro.co.uk/cyber-security/31554/uk-government-lacks-urgency-in-tackling-cyber-security-skills-gap etc – link to UK Digital Strategy and UK Industrial Strategy.

III. Challenges

The ACM general curriculum [3] states 3 Tier-1 and 6 Tier-2 hours for "Information Assurance and Security", but this is the "IAS-only" topics, and ACM expects 32 Tier-1 and 31.5 Tier-2 Hours for IAS topics embedded in other Knowledge Areas.

The UK's official knowledge resource, the CyBOK project [27], has produced reference documentation for some (2 final, 3 for comment out of a planned total of 19) knowledge areas, which are useful references for the experienced educator looking for a definition or characterisation, but a long way from being a textbook (which is not their aim).

Is teaching cybersecurity different? Lecturing is probably not the best way. Should we use real-life case studies (e.g. British Airways [28]).

Should we be teaching it because it's underpinning? because there's a skill shortage? JHD would argue both.

A. PCI DSS

The Payments Card Industry Data Security Standards [20] underpin all processing of credit/debit cards. Nevertheless, they are very rarely mentioned in generalist computer scientist courses — one payments industry person commented “I’ve given up even asking if recruits have heard of PCI DSS: it’s so rare”.

This would not matter so much if everyone handling payments data were sent by their employers on an effective[3] PCI DSS course. However, the payments business is now so spread across websites, often run by SMEs, or non-specialists, that some provision should be made in courses. Even larger enterprises are not immune: [28] reports that the recent British Airways breach was caused by a failure to adhere to PCI DSS in the website maintenance.

B. Educational Resources: SQL Injection

It is 15 years since [29] wrote “All the topics listed above should be presented in the first Database Course”, and the first such topic was SQL injection [30], [31]. SQL injection as an attack has been around for twenty years [32], has its own cartoon (https://xkcd.com/327/, dating back to 2007 according to the Internet Archive) and website (http://bobby-tables.com/). Nevertheless SQL injection is still a major weakness: number one in the OWASP Top 10 [33], and has been in the Top 10 since at least 2003. [34, the UK’s definitive reference] states “a wide range of attack techniques for exploiting SQL injection or script injection are known and documented.”.

Clearly such a major weakness should be well-taught. One would like to think it is, but the first author has yet to meet a UK undergraduate who recalls being taught it *outside* a specialist cybersecurity course. In general it’s hard to determine what is taught, but a reasonable proxy for this is the content of recomended textbooks.

Hence [35] analyzed the database textbooks used by 44 of the top 50 Computer Science departments in the United States (using [36]’s list, the other six didn’t have a book listed). There were seven such books, but three accounted for the 36 of the 44. Five of the seven (30 of the 44) had no mention of SQL injection. On the other two, the more popular one has a seriously flawed discussion[4], and the other, while generally excellent, had a presentational problem[5].

This blindness is not limited to textbooks: although Wikipedia has an excellent article on SQL Injection, it was not linked from the SQL page itself.[6]

C. Informal Resources

The web abounds with informal resources: tutorials and code snippets. How good are these, and how good are people at using these? This has been looked at by [37], who took the top five results from Google for six queries. Of these 30 tutorials, 6 had SQL injection weaknesses, and 3 had Cross-Site Scripting[7] weaknesses. Searching for these fragments in PHP projects on GitHub found 82 instances of these fragments, of which 117 were verified manually to be vulnerable — 80% of which were vulnerable to SQL injection.

D. The case of Java

To the best of the authors’ knowledge, no survey equivalent to [35] has been done for Java textbooks. Indeed, many such books go nowhere near security applications. 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. [38] analysed 503 cybersecurity-related postings on the popular Stack overflow (https://stackoverflow.com) resource. 53% were about the Spring Security framework (https://projects.spring.io/spring-security/), dominated by authentication (45%). The discussion [38, §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 they 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 (16 January 2018) there were no negative comments about this disabling of a vital security feature.

This research was further developed by [39] (and popularised in a security community in [40]). 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%].

E. Android

[41] looked specifically at the use of resources from Stack Overflow in Android applications. Their key finding was this.

> 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.

We should note two caveats (in opposite directions). Their labelling was conservative, in that snippets were only labelled

[3] “Effective” is important: the Processing Director at one major acquirer commented “I just caught two developers in the elevator discussing how to meet a customer requirement, and I had to tell them this was contrary to PCI DSS. Their response was that the customer wanted it!”.

[4] “However, they imply that using parameters is equivalent to using a function to add escape characters around user input. This is incorrect, as using parameters allows SQL statements to be pre-compiled, and prevents any user input from being interpreted as code, while escaping user input is not recommended as a sole defense since imperfect escape functions can easily be subverted.” [35]

[5] “However, the fact that the first example should not be used is not discussed until two pages after the example in the text, and is not mentioned at all in the caption or on the page where the figure appears. This means a student who is skimming the text looking for an example to modify for their own code could simply copy the code that first appears in the example, without being aware that this is in fact an example of what they shouldn’t do.” [35]

[6] The authors intend to fix this after the paper is processed, so as not to break anonymity.

[7] Number 7 in OWASP’s Top Ten [33].

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 [42, Slide 29]. Their key recommendation [42, Slide 32] is "Improve documentation: Clarify what you can(not) copy/paste".

F. Agile

To the best of the authors' knowledge, no survey equivalent to [35] has been done for "Agile" textbooks. It is the authors' experience that the vast majority of students' individual software projects are developed on Agile lines. Many authors have found disconnects between Agile practices and secure software development: notably [21] for small projects and [19] for large projects.

Agile's preference for functionality over non-functional requirements is clearly displayed in practice. [43] 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.

G. Staff

It is well known that cybersecurity skills are in short supply, for example [44].

> Research into the state of IT conducted annually by ESG[8] has revealed that the skills gap in information security continues to widen and has doubled in the past five years. In 2014, 23% of respondents to the survey stated that their organisation had a problematic shortage of information security skills. This had climbed to 51% at the beginning of this year. Clearly, this is an issue which is being felt across many industries and organisations, and is a concern which extends beyond IT leadership into the boardroom.

The ESG survey is international, but ESG have confirmed that the UK figures are very similar.

In the authors' experience, it is proving very difficult to recruit academic staff with specialisms in cybersecurity. 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. A recent example had a professor of cybersecurity, two senior academic positions and 2 junior academic positions in one advert. There are examples in the UK of cybersecurity lecturing jobs remaining unfilled for longer than a year. There are also examples of cybersecurity subject groups moving en masse from one university to another.

IV. Accreditation: RQ3

For a few years now there has been a recognized need in the UK to build knowledge, skills and capacity in the area of cybersecurity. This need has led to the establishment of a number of initiatives from a number of national governments for example The UK Cyber Security Strategy. [45] or National Initiative for cybersecurity Education (NICE) in the USA [46].

The teaching of cybersecurity in higher education pre-dates these initiatives and there has been recognition of the need for the inclusion of cybersecurity as part of the Computer Science discipline for a number of years [47]. There has been a debate as to whether cybersecurity is distinct discipline from Computer Science [48]. The consensus now is that cybersecurity is both a discipline in its own right and that cybersecurity should be taught within Computer Science and related degrees. There have been a number of international initiatives international to define curricula to support this for example Computer Science Programmes [3, which added "Information Assurance and Security" for the first time] and specialised cybersecurity Programmes [22].

In the United Kingdom, Higher Education provision addresses both approaches. A significant number of undergraduate and postgraduate programmes are available in both the areas of Computer Science and cybersecurity (and closely related fields Computer Security, Digital / Computer Forensics, etc). In the UK, Universities and Colleges Admissions Service (UCAS) lists over 40 Higher Education Institutes (HEI) providing Undergraduate qualifications related to cybersecurity for entry in September 2019. An even larger number of HEI provide study opportunities related to more general Computer Science. UCAS lists 246 provides for undergraduate programmes related to Computer Science.

Accreditation has evolved to directly addresses the cybersecurity challenges in both general Computer Science programmes and specialist cybersecurity programmes. In the UK, accreditation in the broad computing area is being performed by a few different agencies. These include:

1. Not for Profit Organisations Tech Partnership Degrees is a Not For Profit Organisation that provides endorsements to Higher Education programmes with specific curricula elements aimed at job market requirements. One of the curricula elements is related to cybersecurity. Tech Partnership Degrees have a specialist scope, endorsing programmes in the area of IT Management for Business and Software Engineering for Business. Tech Partnership Degrees currently endorse 14 IT Management for Business Programmes and 5 Software Engineering for Business Programmes. As such Tech Partnership Degrees currently have limited impact upon more general Computer Science education and none upon specialist cybersecurity education.

The Institute of Coding is a not for profit organisation that intends to enhance how Digital Skills are developed in Higher Education in the UK [26]. This is likely to include

[8] Apparently https://www.esg-global.com/research/esg-brief-2018-cybersecurity-spending-trends.

cybersecurity related skills. Like the Tech Partnership the focus is upon job market requirements. Additionally the Institute is looking at potentially endorsing the demonstrable capabilities of graduates as shown by their university studies, work experience and work placements. Given the size of this initiative this potentially has a significant role to play however at time of writing it is clearly a work in progress.

2. National Cyber Security Centre (NCSC) The NCSC is a UK Government organisation tasked with enhancing the cybersecurity of the UK. The NCSC publishes and accredits to a number of cybersecurity standards [49]. These standard are linked to the ACM recommendations for curricula. To date the major focus of NSSC accreditation has been upon Masters degrees specializing in cybersecurity. More recently the NCSC has also began accrediting integrative masters programmes, undergraduate degrees in cybersecurity and Computer Science degrees with a significant cybersecurity focus [50].

Currently accredited are 15 cybersecurity MSc programmes with a further 11 provisional accredited, 3 integrated masters cybersecurity programmes and 1 cybersecurity Degree Programme with a further 2 provisionally accredited. Hence the extent of accreditation is currently reasonably limited in terms of reach to Computer Science programmes. This appears to be a positive initiative that will hopefully further develop over time.

3. Professional Bodies The BCS, The Chartered Institute for IT (BCS) and the Institution of Engineering and Technology (IET) both accredit programmes in the general area of Computer Science and the more specialist area of cybersecurity discipline areas. The accreditation provided by these institutes are underpinned by international Initiatives such as the Washington Accord[9] and Seoul Accord[10]. These memoranda support the internationalising of the curriculum and promote consistency and parity in Computer Science Education globally. These professional bodies are also registered charities and hence have responsibilities for public good which extends beyond short term job market needs [51], [52]. Both the IET and The BCS have a long history of expecting coverage environmental factors within the programmes they accredit. The BCS has for a number of years been expecting significant coverage of Legal, Ethical, Social and Professional Issues [53]. Clearly cybersecurity has been and continues to be part of these expectations.

In recent years the BCS has evolved its Accreditation Practices to promote and mandate the inclusion of cybersecurity within the programmes the body accredits. The timeline which this process has followed in Table I.

IV. ACCREDITATION:RQ3 - A. Developing Expectations	
UK Government Cybersecurity Strategy [45]	November 2011
Three workshops of a consortium of industry, academia and government bodies - led by CPHC and (ISC)2 - leading to the development of Cybersecurity learning guidelines to be embedded into BCS accredited UK Computer Science and IT-related degree [54]	2013 to June 2015
UK Government report Cybersecurity Skills, Business Perspectives and Government's Next Steps Report Released [55]	March 2014
Council of Professors and Heads of Computing (CPHC) Identifies Cybersecurity as one the top 3 concerns in Computing	April 2014
Joint Development of White Paper from CPHC and The International Information Systems Security Certification Consortium(ISC)2 [56]	April - November 2014
Extended Cybersecurity Criteria included in BCS Accreditation Guidelines [4]	June 2015
IV. ACCREDITATION:RQ3 - B. What does the BCS tell Universities?	
Cybersecurity Principles Roadshow	March-April 2016
IV. ACCREDITATION:RQ3 - C. Accreditation - what progress has been made?	
All visited HEIs expected to be fully compliant	September 2020 (BCS follow a 5-year Accreditation Cycle)

TABLE I
TIMELINE OF THE DEVELOPMENT OF CYBERSECURITY EXPECTATIONS

A. Developing Expectations

Internationally the expectations regarding both the breadth and depth of the expected cybersecurity coverage has been the subject of much discussion, debate and analysis. Like many Governments, the UK Government has been actively been seeking ways to address this [45], [55]. In parallel to the work complete by the ACM [3], in the UK considerable effort was taken to ensure Industry, Higher Education, Government and the related Professional Bodies collaborated on a set of guidelines which are to the benefit of the various stakeholders and wider society [57]. In 2013, an initiative was set up by (ISC)2, CPHC (the representative body of Computer Science Departments) and the Cabinet Office to examine embedding cybersecurity into undergraduate degrees in the UK. Three workshops in 2013 and 2015 attempted to define the principles of cybersecurity education and proposed a framework for embedding these principles in UK Computing Science curricula. Attendees at the workshops included industry, professional bodies, UK government departments and more than 30 Universities that offer undergraduate Computing Science degrees. This work initially lead to a white paper related to a proposal in the form of a white paper [56], followed by a set of guidelines [54]. The BCS agreed to adopt the outputs into their accreditation criteria. This was the first time that cybersecurity has been extensively referenced within accreditation criteria for computing and IT-related degrees. The fact that cybersecurity is included as a component of the BCS accreditation criteria, reflects the importance placed on cybersecurity and the expectation that all computing graduates should have knowledge and skills in cybersecurity as they move towards Chartered status.

The produced reference guidelines ("Cybersecurity Prin-

[9] http://www.ieagreements.org/accords/washington/.

[10] https://www.seoulaccord.org/.

ciples and Learning Outcomes") [54] established a baseline of common knowledge, example learning outcome domains for cybersecurity within the Computing Science courses and guidance on embedding the concepts. The document provides specific guidance for embedding and enhancing relevant cybersecurity principles, concepts and learning outcomes within their undergraduate curricula. The document suggested 5 areas of coverage

- Information and risk
- Threats and attacks
- Cybersecurity architecture and operations
- Secure systems and products; and
- Cybersecurity management

The ambition of this approach is to influence the curricula of all programmes seeking accreditation (regardless of the precise discipline area.) The approach taken is not intended to be prescriptive or stifle innovation, however it is intended to promote curricula that would benefit the students upon programmes, their future employers and wider society. In this context this is realized as an expectation cybersecurity is an inclusion in all degrees accredited by the BCS. e.g. the expectation for coverage is true for Computer Science as well as cybersecurity programmes. Two criteria are expected to be covered by all programmes seeking accreditation. These are [4]:

2.1.6 Recognise the legal, social, ethical and professional issues involved in the exploitation of computer technology and be guided by the adoption of appropriate professional, ethical and legal practices

2.1.9 Knowledge and understanding of information security issues in relation to the design, development and the use of information system

Additionally programmes seeking Chartered Information Technology Professional Accreditation also have to cover:

3.1.2 Knowledge and understanding of methods, techniques and tools for information modelling, management and security

In the context of BCS accreditation, these requirements imply an exit standard that all students on a programme must be able to demonstrate irrespective of the option choices they have made. This means a HEI applying for accreditation is expected to provide evidence that the criteria are taught and assessed in a non-trivial manner, to and by all students upon the programme seeking accreditation . A HEI is expected to provide evidence in the form of programme and module specification documentation and example assessment specifications (coursework and examinations). These criteria and the expectation that they are taught and assessed has been present for a number of years.

The BCS accreditation (2.1.6, 2.1.9 and 3.1.2) is not prescriptive, but encourages HEIs to embed cybersecurity teaching across a range of subject areas in the computer science curriculum such as programming, software design, databases, networking, architecture. In addition there an expectation that there is significant coverage of cybersecurity principles and fundamentals - either as a stand alone module or as a significant component(s) of other modules. This approach differs from the ACM approach where the expectations are more explicit and the curriculum expectations are specified at a more granular level.

B. What does BCS tell Universities

The agreed Cybersecurity Principles and Learning Outcome [54] were discussed with the wider education community by a road-show led by CPHC. A series of workshops took place in 2015 which presented the rationale for embedding cybersecurity in the curriculum of Computing Science degrees. The workshops included case studies from universities who had embedded cybersecurity into their Computer Science curricula illustrating different approaches to implementation. The workshops had 102 attendees from the academic Computing Science community representing 60 UK Universities.

The BCS Guidelines on Course Accreditation are published upon the BCS website [4]. The BCS also publishes the changes that have been made [58]. When changes are made, the BCS communicates the changes by email and in writing to all the BCS Educational Affiliates, that is all the HEIs that seek accreditation from the BCS. The expectations for Cybersecurity were extended in the June 2015 version of the guidelines for consideration at Accreditation Visits that took place from September 2015 or later.

This change to the accreditation guidelines is now in an implementation period. The accreditation process adopted by the BCS is cyclic in nature. Formally, the cycle is 5 years in duration. The new expectations have been implemented as follows. To ensure continuous accreditation, accreditation visits are normally scheduled every 5 years. At the time of the next visit in this accreditation cycle, accreditation is conditional upon a HEI having considered the guidelines and either adjusted the curriculum to meet the new expectations or have a formal plan in place for when and how adjustments will be made. It is anticipated that from 2020 the expectation will be all accredited programmes have the new expectations fully embedded.

In the year prior to an Accreditation Visit, HEIs are invited to an Accreditation Briefing from the BCS. The intention of the briefing is to help ensure Accreditation Visits go smoothly from the perspective of both the BCS and visited HEI. The briefings take place virtually. The briefing includes a summary of the process, discussion of recent changes, guidance regarding the application and a summary of common issues that are being seen in other HEIs. Significant opportunity for seeking clarification is provided. One of the issues that is highlighted is not all institutions have yet evolved their programmes to fully address the increased expectation for cybersecurity. This is resulting in accreditation being contingent upon a HEI taking action to address this short fall or in some cases the withdrawal of accreditation. A number of HEIs are in the process of adjusting their curricula to meet the new expectations. In this case, the BCS notes the changes to programme design, the outputs from which will be scrutinized at the next accreditation visit.

C. Accreditation - what progress has been made

This initiative is a collective attempt to formally include cybersecurity in all BCS Accredited programmes. Some of these programmes will be specialist cybersecurity programmes, however the majority will take a different emphasis. This is a work in progress. A full cycle of accreditation visits has not yet taken place following the adjustment to the BCS Guidelines. What is being observed is the majority of visited HEIs have now either adjusted their curricula to extend the coverage of cybersecurity or have a plan in place to do so. However, a minority are requiring encouragement to do so.

From the start of the Autumn 2015 term, up to and including the Autumn 2018 term, the BCS have carried out 70 accreditation visits (including 4 international visits). The BCS identified action was required to address concerns related to cybersecurity at 16 HEIs. So 54 HEIs were already delivering cybersecurity in keeping with the BCS expectations.

Long term actions were expected from 12 HEIs (6 in 2015/16, 3 in 2016/17 and 3 in the Autumn of 2018) who were awarded 'At Threshold' judgments. 10 of these judgments were across all programmes. 1 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. As indicated earlier, this was commonly the case that adjustments had been made to approved programmes of study, however the adjusted modules had not yet been delivered so the evidence base was incomplete in terms of how cybersecurity was assessed.

Short terms 90 Day Responses where required from 4 HEIs. The outcomes of these actions were as follows:

A) Of the 11 UG programmes involved all were approved 'At Threshold'

B) Of the 9 UG programmes involved, 8 were approved and 1 refused

C) Of the 5 UG programmes involved, all approved 'At Threshold'

D) Of the 3 UG programmes involved, all 3 were refused.

Good practice was identified at one university by the commendation:

> "The second year project provides an opportunity for exploring security aspects in depth with an industrial use case".

In sum, this shows that many UK HEIs have now embedded cybersecurity in their provision, a number are in the process of doing so and a minority have chosen not to. Clearly not all HEIs in the UK necessarily have to apply for accreditation, or apply for accreditation for all their programmes, but even so this is significant evidence of inclusion of cybersecurity to an agreed standard.

V. Conclusions

As regards our research questions, we can make the following comments.

RQ1 The guidelines from both ACM and BCS are good for general education. However, the most important item would seem to be an attitude of caution with respect to both offline (§III-B) and online (§III-D–) resources.

RQ2 The recommendation in [3, p. 98] that cybersecurity be taught largely through other Knowledge Areas is, in abstract, a good idea. Indeed, a recent discussion on cybersecurity had the aerospace engineers amazed that security was a separate topic: "for us, safety is present everywhere". However, in the current state of education resources (sections §III-B–III-D) this may be a counsel of perfection. It is more important that issues like SQL injection [35] or correct use of SSL/TLS [39] be taught somewhere than that they not be taught at all. Nevertheless, we believe it is wrong for a complete curriculum to ignore CyberSecurity issues and:

- teach SQL without teaching SQL Injection ([35] and the second author's experience);
- teach "web programming" without teaching Cross-Site Scripting [33, (XSS)];
- teach `strcpy` etc. without teaching the necessity of guards.

We commend the BCS-identified good practice of exploring cybersecurity via a project, possibly in PCI DSS (§III-A).

RQ3 Accreditation (as practised by BCS) is a valuable tool in improving the standard of cybersecurity teaching, and spreading good practice, and should continue this.

We have the following specific recommendations.

1) Database courses should look carefully at the security aspects of the texts they use, and the examples they quote, on the lines of [35].
2) Web Programming courses should probably do the same, with emphasis on the avoidance of Cross-Site Scripting, and, for production use, the use of a suitable framework[11] that has Cross-Site Request Forgery protection.
3) All computer science courses should emphasise that informal resources should come with a "security health warning": see sections III-C and III-D. One should probably use the data from [39]: "If you pick up a SSL/TLS answer from Stack Overflow, there's a 70% chance it's insecure".

Acknowledgements

Thanks to Sally Pearce, Academic Accreditation Manager, BCS–The Chartered Institute for IT for supplying the summary information related to Accreditation. Many people, accreditors and accredited, contributed to improving the standard of cybersecurity teaching, and spreading good practice.

References

[1] British Airways, "Customer data theft," https://www.britishairways.com/en-gb/information/incident/data-theft/latest-information, 2018.

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

[11] Most modern frameworks do, but this is not often discussed when looking at the advantages of frameworks.

[3] ACM/IEEE-CS Joint Task Force on Computing Curricula, "Computer Science Curricula 2013," ACM Press and IEEE Computer Society Press, Tech. Rep., December 2013. [Online]. Available: http://dx.doi.org/10.1145/2534860

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

[5] T. Crick and S. Sentance, "Computing At School: Stimulating Computing Education in the UK," in *Proceedings of the 11th Koli Calling International Conference on Computing Education Research*. ACM, 2011, pp. 122–123.

[6] N. C. C. Brown, M. Kölling, T. Crick, S. Peyton Jones, S. Humphreys, and S. Sentance, "Bringing Computer Science Back Into Schools: Lessons from the UK," in *Proceedings of the 44th ACM Technical Symposium on Computer Science Education (SIGCSE 2013)*. New York: ACM, 2013, pp. 269–274.

[7] N. C. C. Brown, S. Sentance, T. Crick, and S. Humphreys, "Restart: The Resurgence of Computer Science in UK Schools," *ACM Transactions on Computer Science Education*, vol. 14, no. 2, pp. 1–22, 2014.

[8] S. Arthur, T. Crick, and J. Hayward, "The ICT Steering Group's Report to the Welsh Government," Tech. Rep., September 2013, http://learning.gov.wales/resources/browse-all/ict-steering-groups-report/?lang=en.

[9] F. Moller and T. Crick, "A University-Based Model for Supporting Computer Science Curriculum Reform," *Journal of Computers in Education*, vol. 5, no. 4, pp. 415–434, 2018.

[10] J. H. Davenport, A. Hayes, R. Hourizi, and T. Crick, "Innovative Pedagogical Practices in the Craft of Computing," in *Proceedings of 4th International Conference on Learning and Teaching in Computing and Engineering (LaTiCE 2016)*. Los Alamitos, CA: IEEE Press, 2016, pp. 115–119.

[11] E. Murphy, T. Crick, and J. H. Davenport, "An Analysis of Introductory Programming Courses at UK Universities," *The Art, Science, and Engineering of Programming*, vol. 1(2), no. 18, pp. 18–1–18–23, 2017.

[12] Simon, R. Mason, T. Crick, J. H. Davenport, and E. Murphy, "Language Choice in Introductory Programming Courses at Australasian and UK Universities," in *Proceedings SIGCSE 2018*. New York: ACM, 2018, pp. 852–857.

[13] T. Tryfonas and T. Crick, "Public Policy and Skills for Smart Cities: The UK Outlook," in *Proceedings of 11th International Conference on PErvasive Technologies Related to Assistive Environments (PETRA)*, 2018, pp. 116–117.

[14] A. Parrish, J. Impagliazzo, R. K. Raj, H. Santos, M. R. Asghar, A. Jøsang, T. Pereira, V. J. Sá, and E. Stavrou, "Global perspectives on cybersecurity education," in *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*, ser. ITiCSE 2018. New York, NY, USA: ACM, 2018, pp. 340–341. [Online]. Available: http://doi.acm.org/10.1145/3197091.3205840

[15] Joint Committee [of Parliament] on the National Security Strategy, "Cyber Security Skills and the UK's Critical National Infrastructure: Second Report of Session 2017-19," Houses of Parliament, Tech. Rep. HL Paper 172/ HC 706, 2018. [Online]. Available: https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/706/70605.htm

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

[17] Article 29 Data Protection Working Party, "Guidelines on Data Protection Officers ('DPOs')," http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf, 2016.

[18] N. McCreanor, "Finding the right candidate to be your DPO," https://www.itgovernance.eu/blog/en/finding-the-right-candidate-to-be-your-dpo, 2018.

[19] A. van der Heijden, C. Broasca, and A. Serebrenik, "An empirical perspective on security challenges in large-scale agile software development," in *Proceedings of the 12th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement*, ser. ESEM '18. New York, NY, USA: ACM, 2018, pp. 45:1–45:4. [Online]. Available: http://doi.acm.org/10.1145/3239235.3267426

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

[21] S. Bartsch, "Practitioners' Perspectives on Security in Agile Development," *In International Conference on Availability Reliability and Security*, pp. 479–484, 2011.

[22] Joint Task Force on Cybersecurity Education, "Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity)," https://cybered.hosting.acm.org/wp/wp-content/uploads/2018/02/csec2017_web.pdf, 2017.

[23] R. Ackerman, "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.

[24] R. Ruiz, "A Study of the UK Undergraduate Computer Science Curriculum: A Vision of Cybersecurity," *To appear in 12th International Conference on Global Security*, 2019. [Online]. Available: https://www.cti.gov.br/sites/default/files/images/pdf/artigo-rodrigo-ruiz.pdf

[25] M. Oudshoorn, S. Thomas, R. Raj, and A. Parrish, "Understanding the New ABET Computer Science Criteria," in *Proceedings SIGCSE 2018*. New York: ACM, 2018, pp. 429–434.

[26] J. Davenport, T. Crick, A. Hayes, and R. Hourizi, "The Institute of Coding: Addressing the UK Digital Skills Crisis," in *Proceedings 3rd Computing Education Practice Conference*. ACM, 2019, pp. 10:1–10:4.

[27] University of Bristol Cyber Security Group, "The Cyber Security Body Of Knowledge," https://www.cybok.org/, 2019.

[28] B. Barth, "No fly-by-night operation: Researchers suspect Magecart group behind British Airways breach," https://www.scmagazine.com/home/security-news/no-fly-by-night-operation-researchers-suspect-magecart-group-behind-british-airways-breach/, 2018.

[29] M. Guimaraes, H. Mattord, and R. Austin, "Incorporating security components into database courses," in *Proceedings of the 1st annual conference on Information security curriculum development*. ACM, 2004, pp. 49–52.

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

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

[32] M. Horner and T. Hyslip, "SQL Injection: The Longest Running Sequel in Programming History," *Journal of Digital Forensics, Security and Law*, vol. 12, no. 2, pp. 97–107, 2017.

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

[34] University of Bristol Cyber Security Group, "The Cyber Security Body Of Knowledge: Software Security Knowledge Area Issue 1.0," https://www.cybok.org/, 2018.

[35] C. Taylor and S. Sakharkar, "';DROP TABLE textbooks;– An Argument for SQL Injection Coverage in Database Textbooks," in *Proceedings SIGCSE 2019*, 2019, pp. 191–197.

[36] M. Stanger and E. Martin, "The 50 Best Computer-Science and Engineering Schools in America, 2015," http://www.businessinsider.com/best-computer-science-engineering-schools-in-america-2015-7, 2015.

[37] T. Unruh, B. Shastry, M. Skoruppa, F. Maggi, K. Rieck, J.-P. Seifert, and F. Yamaguchi, "Leveraging Flawed Tutorials for Seeding Large-Scale Web Vulnerability Discovery," https://arxiv.org/pdf/1704.02786.pdf, 2017.

[38] N. Meng, S. Nagy, D. Yao, W. Zhuang, and G. Arango Argoty, "Secure coding practices in java: Challenges and vulnerabilities," in *2018 IEEE/ACM 40th International Conference on Software Engineering (ICSE)*, 2018, pp. 372–383.

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

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

[41] F. Fischer, K. Böttinger, H. Xiao, C. Stransky, Y. Acar, M. Backes, and S. Fahl, "Stack Overflow Considered Harmful? The Impact of Copy&Paste on Android Application Security," in *38th IEEE Symposium on Security and Privacy (SP)*, 2017, pp. 121–136.

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

[43] A. Naiakshina, A. Danilova, C. Tiefenau, M. Herzog, S. Dechand, and M. Smith, "Why Do Developers Get Password Storage Wrong?: A Qualitative Usability Study," *In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17). ACM*, pp. 311–328, 2017.

[44] Michael Page Ltd., "Closing the information security skills gap," https://www.michaelpage.co.uk/our-expertise/technology/closing-information-security-skills-gap, 2018.

[45] UK Cabinet Office, "The UK Cyber Security Strategy," https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf, 2011.

[46] National Initiative for Cybersecurity Education (NICE), "NICE Cybersecurity Workforce Framework," https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework, 2013.

[47] M. Hentea, H. Dhillon, and M. Dhillon, "Towards Changes in Information Security Education," *Journal of Information Technology Education: Research*, vol. 5, pp. 221–233, 2006. [Online]. Available: https://www.learntechlib.org/p/111542/

[48] A. McGettrick, "Toward effective cybersecurity education," *IEEE Security and Privacy*, vol. 11, no. 6, pp. 66–68, 2013.

[49] National Cyber Security Centre, "NCSC degree certification," https://www.ncsc.gov.uk/information/ncsc-degree-certification-call-new-applicants-0, 2018.

[50] ——, "Certification of Bachelor's and Master's Degrees in Cyber Security," 2018. [Online]. Available: https://www.ncsc.gov.uk/content/files/protected_files/article_files/degrees-at-a-glance.pdf

[51] B. Stensaker and L. Harvey, "Old Wine in New Bottles? A Comparison of Public and Private Accreditation Schemes in Higher Education." *Higher Education Policy*, vol. 195, pp. 65–8, 2006.

[52] S. Mutereko, "Analysing the accreditation of engineering education in South Africa through Foucault's panopticon and governmentality lenses." *Assessment & Evaluation in Higher Education*, vol. 43, pp. 235–247, 2017.

[53] P. Brooke, T. Prickett, S. Keogh, and D. Bowers, "Becoming Professional A University Perspective." *ITNow*, vol. 60, pp. 16–17, 2018.

[54] CPHC, ISC^2, "Cybersecurity Principles and Learning Outcomes for Computer Science and IT-Related Degrees)," https://cphcuk.files.wordpress.com/2015/06/j0028-isc2-white-paper-a4-v5-260515lr.pdf, 2015.

[55] UK Cabinet Office, "Cyber security skills: business perspectives and government's next steps," https://www.gov.uk/government/publications/cyber-security-skills-business-perspectives-and-governments-next-steps, 2014.

[56] CPHC, ISC^2, "perspectives: Integrating cybersecurity into computer science curricula," https://cphcuk.files.wordpress.com/2014/11/perspectives_integrating-cybersecurity-into-computer-science-curricula-final31102014.pdf, 2014.

[57] A. Irons, N. Savage, C. Maple, A. Davies, and L. Turley, "Cybersecurity in CS Degrees," *ITNow*, vol. 58, pp. 56–57, 2016. [Online]. Available: https://doi.org/10/1093/itnow/bww053

[58] British Computer Society, "List of Changes made since 2015 v2," https://www.bcs.org/upload/pdf/guidelines-changes-2018.pdf, 2018.