A UK Case Study on Cybersecurity Education and Accreditation

Tom Crick*, James H. Davenport†, Alastair Irons‡ and Tom Prickett§
*Swansea University, Swansea, UK; Email: thomas.crick@swansea.ac.uk
†University of Bath, Bath, UK; Email: j.h.davenport@bath.ac.uk
‡Sunderland University, Sunderland, UK; Email: alastair.irons@sunderland.ac.uk
§Northumbria University, Newcastle upon Tyne, UK; Email: tom.prickett@northumbria.ac.uk

***Abstract*—This Innovative Practice Full Paper presents a national case study-based analysis of the numerous dimensions to cybersecurity education and how they are implemented and accredited; from understanding the interaction of hardware and software, moving from theory to practice (and vice versa), to human factors, policy and politics (as well as other important facets). A multitude of model curricula and recommendations have been presented and discussed in international fora in recent years, with varying levels of impact on education, policy and practice. This paper address three key questions: *i)* What is taught and what should be taught for cybersecurity to general computer science students; *ii)* Should cybersecurity be taught stand-alone or in an integrated manner to general computer science students; and *iii)* Can accreditation by national professional, statutory and regulatory bodies enhance the provision of cybersecurity within a body's jurisdiction?**

Evaluating how cybersecurity is taught in all aspects of computer science is clearly a task of considerable size, one that is beyond the scope of this paper. Instead a case study-based research approach, primarily focusing on the UK, has been adopted to evaluate the evidence of the teaching of cybersecurity within general computer science to university-level students. Thus, in the context of widespread international computer science/engineering curriculum reform, what does this need to embed cybersecurity mean more generally for institutions and educators, and how can we teach this subject more effectively? Through this UK case study, and by contrasting with the US, we demonstrate the positive effect that national accreditation requirements can have, and give some recommendations both for future research and curriculum developments.

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

I. Introduction

Cybersecurity has increasingly been a headline feature in the news over recent years, generally prompted by spectacular breaches, from major credit reference agencies [1], telecoms companies [2], national airlines [3], online dating websites [4], and even between sovereign governments [5]. These major breaches have had significant impact on both individual citizens and society in general, requiring attention from organisations of all sizes [6][1]:

> "*...[need to] 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.*"

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

These global cybersecurity crises have compelled academic institutions to address the demand for educated cybersecurity professionals [7]. As no shared framework for "cybersecurity" as an academic discipline exists, growth has been unfocused and largely driven by training materials, which makes it harder to establish a common body of knowledge (for example, in the UK, the CyBOK project [8] is still a work in progress). An international perspective is harder still, as different nations use different criteria to define local needs [9]. As a result, new programmes entering this space are free to conceptualise, design, package and market their initiatives, as there is no globally accepted reference model for cybersecurity to allow employers or students to understand the extent or ambition of a given cybersecurity program [10], [11].

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, at the individual level and via recommended curricula [12], [13] and professional accreditation requirements [14]. This is further reinforced by a wider focus on digital skills and computer science education reform, especially across the nations of the UK [15], [16], [17].

A recent ACM working group, as part of the Innovation and Technology in Computer Science Education (ITiCSE) conference series [11], has been capturing global perspectives on cybersecurity education, but has yet to report its full findings. An aim of the ITiCSE working group is to develop a taxonomy for approaches to cybersecurity education, resulting in improved standards and goals for many different types of cybersecurity programmes; a further aim is to "catalog existing [...] knowledge materials", but there is no mention of any quality control over these. Nevertheless, it is one thing to write national curricula, specifications and requirements, and another thing to deliver appropriate and relevant education and skills; furthermore, this paper asks how well this is done in practice.

II. 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), but also all in IT need to know *some* cybersecurity – thus, there is a case for depth as well as breadth [18], [19]. This is not a new concern: see [20] for concerns over five years ago, but it is a growing one.

This need to build knowledge, skills and capacity in the area of cybersecurity has also led to the establishment of a number of strategic policy initiatives from a number of national governments, for example the UK's Cyber Security Strategy [21] (as well as the setting up of the UK National Cyber Security Centre, with increased scrutiny of what this means for the UK's critical national infrastructure [22]; also initiatives such as Cyber Essentials[2]), the EU Cybersecurity Act [23] (which reinforces the mandate of the EU Agency for Cybersecurity – ENISA – the European Union Agency for Network and Information and Security), or the National Initiative for Cybersecurity Education (NICE) in the USA [24].

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 discipline of computer science for a number of years [25], [9]. There have been a number of international initiatives to define curricula to support this, for example the ACM Computer Science Curricula Recommendations [26, which added "Information Assurance and Security" for the first time], as well as for specialised cybersecurity degree programmes [27]. There has been a debate as to whether cybersecurity is distinct discipline from computer science [7]. The consensus increasingly is that cybersecurity is both a discipline in its own right and that cybersecurity should be taught within computer science and related degrees. Recent evolution of cybersecurity education shows that it has begun to take shape as a true academic perspective, as opposed to simply being a training domain for certain specialised jobs. More recent work presents cybersecurity as a "meta-discipline"; that is, cybersecurity should be used as an aggregate label for a wide variety of similar disciplines, much in the same way that the terms "engineering" and "computing" are commonly used [28].

Further to the substantial computer science and digital skills curriculum reform across the UK [29], [15], [17], the question is raised whether cybersecurity should be formally taught in schools, as part of a compulsory education. While aspects of "e-safety" and principles of protecting personal data are increasingly visible in formal curricula [30], the majority of UK schoolchildren's exposure to cybersecurity skills is through national extra-curricular competitions, for example Cyber Security Challenge UK[3]. The Institute of Coding [31], a £40m+ initiative by the UK Government to transform the digital skills profile of the country – but primarily focused on university graduates – does indeed mention cybersecurity, but merely as a sub-item in one work package.

[2]Cyber Essentials is a UK Government-backed, industry-supported scheme to help organisations protect themselves against common online threats: https://www.cyberessentials.ncsc.gov.uk

[3]https://www.cybersecuritychallenge.org.uk

III. Research Questions

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

(i) The general public — this is important, but there are many initiatives in this area, which are, rightly, largely separated from computing education.
(ii) The generalist computer science graduate.
(iii) The generalist computer science masters graduate.
(iv) The specialist computer science graduate.
(v) The specialist computer science masters graduate.

The focus of this paper is on (ii)–(iii): the general computer science graduate.

This paper thus focuses on three research questions:

RQ1 *What cybersecurity is taught and what cybersecurity should be taught to the general computer science students?*

RQ2 *Should cybersecurity be taught stand-alone or in an integrated manner to general computer science students?*

RQ3 *Can accreditation by professional, statutory and regulatory bodies (PSRBs) enhance the provision of cybersecurity within a body's jurisdiction?*

A. Research Approach

A UK-focused case study-based approach is adopted in this project. As is common in case study-based research, many alternative case studies could have been chosen. The cases are illustrative rather than comprehensive in terms of the available case studies or challenges. The cases were evaluated to articulate the progress made and highlight opportunities for future developments in education and practice.

The first set of cases that are considered are the current situation in terms of recommendations from a sample of relevant PSRBs, together with the published evidence regarding compliance with these recommendations. This is followed by the evaluation of the policy context. Together these provide a context to the ongoing enhancement initiatives in the area of cybersecurity education.

In order to address *RQ1* and *RQ2* a number of case studies pertaining to challenges of delivering cybersecurity to undergraduate computer science students are evaluated. Namely, an industry problem with evident cybersecurity implications; the current state of educational resources with respect to cybersecurity; and the challenges evident in the UK related to the recruitment and retention of suitably qualified academic staff in the cyber security area.

Finally, in order to address *RQ3* cases studies are evaluated related to the challenges and successes of PSRB accreditation of cybersecurity in undergraduate computer science in one jurisdiction (the UK). As discussed in the current situation section, in this jurisdiction mandating cybersecurity within PSRB accreditation is at a reasonably mature stage.

B. Current State of Play

The ACM/IEEE-CS Joint Task Force on Computing Curricula [26, p. 97] takes a distinct view on the Knowledge Areas (KAs) related to 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 KAs*

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

Nevertheless, the situation on the ground in the USA is different [32]:

> *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.*

The UK situation is distinctly different: 61% of UK courses offer mandatory cybersecurity content, and this research was based on web scraping [33, Table 1]. As such it represents a lower bound since not all coverage will necessarily be clearly articulated in publicly available documentation online.

It is at least plausible to attribute this difference to differences in the accreditation regimes, as the external circumstances, governmental pressures, and professional body/learned society curricula are all similar.

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 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, 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*" [14, p. 30] since 2010 with an enhanced cybersecurity related definition of what this entails since 2015 [14, p. 17–18].

US ACM has equally had cybersecurity ("Information Assurance and Security" — IAS) in the curriculum since 2013 [26], 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 [34, 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).

IV. Challenges: *RQ1* and *RQ2*

The ACM Computer Science Curricula Recommendations [26] states three Tier-1 and six 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 body of knowledge resource, the CyBOK project[8], has produced reference documentation for some (as of June 2019: five final, seven 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).

A. Industry Standards: PCI DSS

Is teaching cybersecurity different? Lecturing is probably not the best way. Should we use real-life case studies (e.g. British Airways [35]). [36] suggests that there are benefits from teaching this discipline area in a more practical manner. There are a number of ways a more practical manner could be action, one would be by the inclusion of pertinent cybersecurity standards in the curricula.

The Payments Card Industry Data Security Standards (PCI DSS) [37] is one such standard. PCI DSS underpins all processing of credit/debit cards. Nevertheless, they are 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: [35] reports that the recent British Airways breach was caused by a failure to adhere to PCI DSS in the website maintenance.

It is an interesting question as to whether standards such as PCI DSS should be addressed within degree courses (clearly degree courses can never cover all standards) or whether they should be addressed in professional training courses. However it appears the current situation is not ideal from the perspective of industry (or users of systems) and the inclusion of pertinent standards could be seen as a useful enhancement activity to the coverage of cybersecurity within generalist computer science courses.

B. Educational Resources

1) SQL Injection: It is 15 years since [38] wrote "All the topics listed above should be presented in the first Database Course", and the first such topic was SQL injection [39], [40]. SQL injection as an attack has been around for twenty years [41], 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 Open Web Application Security Project (OWASP) Top 10 [42], and has been in the Top 10 since at least 2003. [43, 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. In general it is hard to determine what is taught, but a reasonable proxy for this is the content of recommended textbooks.

Hence [44] analysed the database textbooks used by 44 of the top 50 computer science departments in the USA. 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. 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 oversight is not limited to textbooks: although Wikipedia has an article on SQL Injection, it was not linked from the SQL page itself.[6]

2) The Case of Java: A recommendation for future work is a comprehensive survey equivalent to [44] 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. [45] 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 [45, §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 (16 January 2018) there were no negative comments about this disabling of a vital security feature.

This research was further developed by [46] (and popularised in a security community in [47]). 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) Android: A recommendation for future work is a comprehensive survey equivalent to [44] for Android textbooks; [48] looked specifically at the use of resources from Stack Overflow in Android applications. The 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.*

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 [49, Slide 29]. Their key recommendation [49, Slide 32] is "*Improve documentation: Clarify what you can(not) copy/paste*".

4) Agile: A recommendation for future work is a comprehensive survey equivalent to [44] for "Agile" textbooks. Many authors have found disconnects between Agile practices and secure software development: notably [50] for small projects and [51] for large projects.

Agile's preference for functionality over non-functional requirements is clearly displayed in practice. [52] 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.

5) 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 [53], This research took the top five results from Google for six queries. Of these 30 tutorials, six had SQL injection weaknesses, and three had Cross-Site Scripting[7] 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, a recommendation of future work is to explore and evaluate students' (and indeed others') use of such informal resources.

C. Staff

It is well known that cybersecurity skills are in short supply [9]. For example:

> *Research into the state of IT conducted annually by Enterprise Strategy Group (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.* [54]

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

[4] "*However, the paper implies 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.*" [44]

[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.*" [44]

[6] Fixing this is a suggestion for future work.

[7] Number 7 in OWASP's Top Ten [42].

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

In the UK, there is a prominence of job adverts 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. 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 subject groups moving en masse from one university to another.

V. Accreditation by PSRBs: *RQ3*

In the UK as in most jurisdictions, higher education provision addresses general computer science and specialist cybersecurity courses. 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, the Universities and Colleges Admissions Service (UCAS) lists over 40 higher education institutions providing undergraduate qualifications related to cybersecurity for entry in September 2019. An even larger number of institutions 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 five 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 entity, led by the University of Bath, that intends to enhance how digital skills are developed in higher education in the UK [31]. This is likely to include 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 [55]. These standards are linked to the ACM recommendations for curricula [26]. To date the major focus of NCSC accreditation has been upon Masters degrees specialising 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 [56].

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/Learned Societies

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 the 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 [57], [58]. Both the BCS and the IET have a long history of expecting coverage of environmental factors within the programmes they accredit. The BCS has for a number of years been expecting significant coverage of what it terms *Legal, Ethical, Social and Professional Issues* [59]. 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.

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 [61], [21]. In parallel to the work complete by the ACM [26], in the UK considerable effort was taken to ensure industry, higher education, government

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

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

TABLE I
TIMELINE OF THE DEVELOPMENT OF CYBERSECURITY EXPECTATIONS

IV. ACCREDITATION (*RQ3*) - A. Developing Expectations	
UK Government Cybersecurity Strategy [21]	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 [60]	2013 to June 2015
UK Government report Cybersecurity Skills, Business Perspectives and Government's Next Steps Report Released [61]	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 $(ISC)^2$ [62]	April - November 2014
Extended Cybersecurity Criteria included in BCS Accreditation Guidelines [14]	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 institutions expected to be fully compliant (BCS follow a 5-year Accreditation Cycle)	September 2020

and the relevant professional bodies collaborated on a set of guidelines which are to the benefit of the various stakeholders and wider society [63]. In 2013, an initiative was set up by $(ISC)^2$, CPHC (the representative body of UK computer science departments) and the UK 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 computer science curricula. Attendees at the workshops included industry, professional bodies, UK government departments and more than 30 Universities that offer undergraduate computer science degrees. This work initially lead to a white paper related to a proposal in the form of a white paper [62], followed by a set of guidelines [60]. 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 Principles and Learning Outcomes*") [60] established a baseline of common knowledge, example learning outcome domains for cybersecurity within the computer 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 realised 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 [14]:

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 (CITP) 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 an institution 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. An institution 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 institutions 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 Are Universities Told?

The agreed Cybersecurity Principles and Learning Outcome [60] 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 computer 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 computer science community representing 60 UK Universities.

The *BCS Guidelines on Course Accreditation* are published online [14]. The BCS also publishes the changes that have been made [64]. When changes are made, the BCS communicates the changes by email and in writing to all the BCS Educational Affiliates, that is all the institutions 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 five 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 an institution 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, institutions are invited to a briefing from the BCS. The intention of the briefing is to help ensure accreditation visits are successful from the perspective of both the BCS and the institution. 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 institutions. 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 an institution taking action to address this short fall or in some cases the withdrawal of accreditation. A number of institutions 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 scrutinised 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 institutions 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 four international visits). The BCS identified action was required to address concerns related to cybersecurity at 16 institutions. So 54 institutions were already delivering cybersecurity in keeping with the BCS expectations.

Long-term actions were expected from 12 institutions (six in 2015/16, three in 2016/17 and three in Autumn 2018) who were awarded '*At Threshold*' judgments. Ten 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. 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 four institutions; the outcomes of these actions were as follows:

- Of the 11 UG programmes involved all were approved '*At Threshold*';
- Of the 9 UG programmes involved, 8 were approved and 1 refused;
- Of the 5 UG programmes involved, all approved '*At Threshold*';
- 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 institutions 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 institutions 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.

VI. Conclusions and Future Work

The work presented in this paper is a first step towards better understanding the nature, design, structure and assessment of cybersecurity education in the UK, through the lens of accreditation. It is clear that professional body accreditation is having a positive effect on universities, supporting wider national policy imperatives. It is also clear that there is a significant need for mobilising the international computer science academic community – alongside some of the existing

initiatives presented at the start of this paper – to continue this focus on cybersecurity education, and provide international comparators, portability and sharing of best practice.

As regards to the three research questions:

RQ1: What cybersecurity is taught and what cybersecurity should be taught to the general computer science students?

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 (§IV-B1) and online (§IV-B2) resources.

RQ2: Should cybersecurity be taught stand-alone or in an integrated manner to general computer science students?

The recommendation in [26, p. 98] that cybersecurity be taught largely through other Knowledge Areas is, in abstract, a good idea. However, in the current state of education resources (sections §IV-B) may be a counsel caution in this approach. It is more important that issues like SQL injection [44] or correct use of SSL/TLS [46] be taught somewhere than that they not be taught at all. Nevertheless, it is wrong for a complete curriculum to ignore cybersecurity issues for example

- teach SQL without teaching SQL Injection [44];
- teach "web programming" without teaching Cross-Site Scripting [42, (XSS)];
- ignore the impact of GDPR upon systems development;
- uncritically teach the use of Agile Development to develop secure systems.

The BCS-identified good practice of exploring cybersecurity via a project referencing Industry Standards, possibly PCI DSS, is commended (§IV-A).

RQ3: Can accreditation by PSRBs enhance the provision of cybersecurity within a body's jurisdiction?

Accreditation (as practised by BCS in the UK) is a valuable tool in improving the standard of cybersecurity teaching, and disseminating good practice, and should continue this. The time-lag in adoption of cybersecurity in the US seems to be caused by the accreditation differences more than any other factors.

We also 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 [44].
2) Web Programming courses should 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) A study similar to [44] is recommended for future work in Web Programming, Agile Development, Android Development and potentially other areas of the curriculum.
4) All computer science courses should emphasise that informal resources should come with a "security health warning": see sections IV-B5 and IV-B2. One should probably use the data from [46]: "*If you pick up a SSL/TLS answer from Stack Overflow, there's a 70% chance it's insecure*".

[11]Most modern frameworks do, but this is not often discussed when looking at the advantages of frameworks. Even Mozilla's tutorial (https://developer.mozilla.org/en-US/docs/Learn/Server-side/First_steps/Web_frameworks) is silent.

ACKNOWLEDGEMENTS

Thanks to 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 improving the standard of cybersecurity teaching in the UK, and spreading good practice.

N.B. The first two authors are current Vice-Presidents of BCS, The Chartered Institute for IT, and the third and fourth are past and present Chairs of the BCS Academic Accreditation Committee, providing significant personal insight into the UK's national accreditation policy and procedures.

REFERENCES

[1] Equifax, "Cybersecurity incident – information for UK consumers," https://www.equifax.co.uk/incident.html, 2017.

[2] The Guardian, "TalkTalk hit with record £400k fine over cyber-attack," https://www.theguardian.com/business/2016/oct/05/talktalk-hit-with-record-400k-fine-over-cyber-attack, 2016.

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

[4] Wikipedia, "Ashley Madison data breach," https://en.wikipedia.org/wiki/Ashley_Madison_data_breach, 2015.

[5] UK National Cyber Security Centre, "Reckless campaign of cyber attacks by Russian military intelligence service exposed," https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed, 2018.

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

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

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

[9] F. B. Schneider, "Cybersecurity Education in Universities," *IEEE Security and Privacy*, vol. 11, no. 4, pp. 3–4, 2013.

[10] A. Conklin, R. E. Cline, and T. Roosa, "Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors," in *Proc. of 47th Hawaii Int. Conf. on System Sciences*. IEEE, 2014.

[11] 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 *Proc. of ITiCSE 2018*. ACM, 2018.

[12] A. McGettrick, L. N. Cassel, M. Dark, E. K. Hawthorne, and J. Impagliazzo, "Toward curricular guidelines for cybersecurity," in *Proc. of SIGCSE 2014*. ACM, 2014, pp. 81–82.

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

[14] BCS, The Chartered Institute for IT, "Guidelines on course accreditation (May 2018)," http://www.bcs.org/content/ConMediaFile/30202, 2018.

[15] 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.

[16] 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. 1–23, 2017.

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

[18] D. Manson and R. Pike, "The case for depth in cybersecurity education," *ACM Inroads*, vol. 5, no. 1, pp. 47–52, 2013.

[19] J. H. Davenport, A. Hayes, R. Hourizi, and T. Crick, "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, 2016, pp. 115–119.

[20] 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.

[21] UK Cabinet Office, "National Cyber Security Strategy 2016 to 2021," https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021, 2016.

[22] Joint Committee on the National Security Strategy, "Cyber Security Skills and the UK's Critical National Infrastructure," UK Parliament, Tech. Rep., 2018, https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/706/70602.htm.

[23] European Commission, "Cybersecurity Act," https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en, 2018.

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

[25] 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.

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

[27] ACM/IEEE/AIS/IFIP Joint Task Force on Cybersecurity Education, "Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity," 2017.

[28] A. Parrish, J. Impagliazzo, R. K. Raj, H. Santos, M. R. Asghar, A. Jøsang, T. Pereira, and E. Stavrou, "Global perspectives on cybersecurity education for 2030: a case for a meta-discipline," in *Proc. of ITiCSE 2018*. ACM, 2018, pp. 36–54.

[29] S. Arthur, T. Crick, and J. Hayward, "The ICT Steering Group's Report to the Welsh Government," Tech. Rep., September 2013.

[30] 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.

[31] J. Davenport, T. Crick, A. Hayes, and R. Hourizi, "The Institute of Coding: Addressing the UK Digital Skills Crisis," in *Proc. of 3rd Computing Education Practice Conf.* ACM, 2019.

[32] 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.

[33] R. Ruiz, "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, 2019.

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

[35] 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.

[36] R. Weiss, J. Mache, and E. Nilsen, "Top 10 hands-on cybersecurity exercises," *Journal of Computing Sciences in Colleges*, vol. 29, no. 1, pp. 140–147, Oct. 2013.

[37] 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.

[38] M. Guimaraes, H. Mattord, and R. Austin, "Incorporating security components into database courses," in *Proc. of 1st Annual Conf. on Information Security Curriculum Development*. ACM, 2004, pp. 49–52.

[39] 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.

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

[41] 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.

[42] 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.

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

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

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

[46] 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.

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

[48] 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.

[49] 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.

[50] S. Bartsch, "Practitioners' Perspectives on Security in Agile Development," in *Proc. of Int. Conf. on Availability Reliability and Security*, 2011, pp. 479–484.

[51] A. van der Heijden, C. Broasca, and A. Serebrenik, "An empirical perspective on security challenges in large-scale agile software development," in *Proc. ESEM'18*. ACM, 2018, pp. 45:1–45:4.

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

[53] 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," in *Proc. of 11th USENIX Workshop on Offensive Technologies (WOOT 2017)*, 2017.

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

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

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

[57] 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.

[58] 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.

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

[60] 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.

[61] 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.

[62] 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.

[63] A. Irons, N. Savage, C. Maple, A. Davies, and L. Turley, "Cybersecurity in CS Degrees," *ITNow*, vol. 58, pp. 56–57, 2016.

[64] BCS, The Chartered Institute for IT, "List of Changes made since 2015 v2," https://www.bcs.org/upload/pdf/guidelines-changes-2018.pdf, 2018.