

Cybersecurity Is Too Important To Be Left To The Specialists

Tom Crick
Swansea University
Swansea, United Kingdom
thomas.crick@swansea.ac.uk

Alastair Irons
Sunderland University
Sunderland, United Kingdom
alastair.iron@sunderland.ac.uk

James H. Davenport
University of Bath
Bath, United Kingdom
j.h.davenport@bath.ac.uk

Tom Prickett
Northumbria University
Newcastle upon Tyne, United Kingdom
tom.prickett@northumbria.ac.uk

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). Whilst various model curricula and associated recommendations have been presented and discussed in recent years, in this paper we attempt to address the questions “what should the generalist computer scientist 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 to develop in professional practice, sometimes called “information assurance” in the UK and Europe, which worked, even if not well, in a waterfall model.

In the world of software and systems development, we have seen the disruption of Agile (invented 2001) and DevOps (invented 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 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 and global challenge in computing education by analysing the UK perspective on cybersecurity education, with a substantial national security, economic, and skills policy context, shaping the practical considerations for education professionals from schools through to universities. Through this analysis of policy and practice in the UK, we make a number of recommendations for future cybersecurity educational initiatives, including practical suggestions for educators and curriculum designers, with a view for potential adoption and adaption in other jurisdictions.

KEYWORDS

TBC

ACM Reference format:

Tom Crick, James H. Davenport, Alastair Irons, and Tom Prickett. 2019. Cybersecurity Is Too Important To Be Left To The Specialists. In *Proceedings of The 24th Annual Conference on Innovation and Technology in Computer Science Education, Aberdeen, UK, Jul. 15-17, 2019 (ITICSE '19)*, 6 pages. <https://doi.org/10.1145/nnnnnnn.nnnnnnn>

1 INTRODUCTION

Cybersecurity has been in the news for several years, generally prompted by spectacular breaches of one kind or another, such as [5]. 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. [17]¹

There are calls for education to respond to this situation, which it does both at the individual level and via recommended curricula [1] and professional accreditation requirements [6]. There has been a recent international working group [31], 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 3.2).

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

1.1 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: [21] 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 [30]

AI: GDPR essentially expects CyberSecurity to be in all coding. JHD: PCI DSS insists on a Web Application Firewall, which is only needed if you don't trust your applications.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

ITICSE '19, Jul. 15-17, 2019, Aberdeen, UK

© 2019 Copyright held by the owner/author(s). Publication rights licensed to Association for Computing Machinery.

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM...\$15.00

<https://doi.org/10.1145/nnnnnnn.nnnnnnn>

¹Former Director of GCHQ: Brittain equivalent of NSA.

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.

1.2 Research Questions

- (1) The person in the street — probably not. (*interesting point from a public engagement/science communication perspective – aren’t “we” trying to create a digitally competent and capable citizenry? Minor point but maybe worth mentioning e.g. being safe online, accessing public services, etc*)

JHD This is important, agreed, but I think this is being a user: think car driving rather than car design. BUT the point I heard from the WC Engineers “how can security be an option — safety certainly isn’t” is also relevant.

- (2) The general CS graduate.
- (3) The general CS masters graduate.
- (4) The specialist CS graduate.
- (5) The specialist CS masters graduate.

2 POLICY CONTEXT

Substantial CS/digital curriculum reform across the UK [3, 8, 9, 14, 26] – but what about focus on cybersecurity?

UK national economic skills priority e.g. <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021> (especially [21] 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.

3 CHALLENGES

What should be in the general curriculum. Pervasive (as in Maths or LSEPI) rather than specialist option. **JHD to research ACM general curriculum;**

The UK’s official knowledge resource, the CyBOK project [39], 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)

AI noted the workshops with ISC², with the “this is a fad” concept. **AI to write up.** Should we be teaching it because it’s underpinning? because there’s a skill shortage? JHD would argue both.

3.1 PCI DSS

[32].

Alastair to write about their Credit Fraud experience (MSc CyberSecurity). HE Academy grant (to be referenced).

3.2 Educational Resources: SQL Injection

It is 15 years since [16] wrote “All the topics listed above should be presented in the first Database Course”, and the first such topic was SQL injection [2, 34]. SQL injection as an attack has been around for twenty years [19], 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 [28], and has been in the Top 10 since at least 2003. [38, 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 cyber-security course. In general it’s hard to determine what is taught, but a reasonable proxy for this is the content of recommended textbooks.

Hence [36] analyzed the database textbooks used by 44 of the top 50 Computer Science departments in the United States (using [35]’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 discussion², and the other, while generally excellent, had a presentational problem³.

3.3 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 [40], 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 Scripting⁴ weaknesses. Searching for these fragments in PHP projects on GitHub found 82 instances of these fragments, of which 117 were verified by manual to be vulnerable — 80% of which were vulnerable to SQL injection.

3.4 The case of Java

To the best of the authors’ knowledge, no survey equivalent to [36] 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. [24] 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 [24, §4.3.1] of cross-site request forgery (CSRF) is especially worrying. By default, Spring implicitly enables protection against this. But all

²“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.” [36]

³“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.” [36]

⁴Number 7 in OWASP’s Top Ten [28].

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.

[12, 15, 41]

3.5 Staff

It is well known that CyberSecurity skills are in short supply, for example [25].

Research into the state of IT conducted annually by ESG⁵ 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.

JHD possibly to write about his recruitment experiences. ? more IoC input?

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.

Not sure if we want to raise something about funding of posts ??
Poaching of staff ??

Is this too contentious

JHD to ? Poll CPHC, and/or survey job adverts.

3.6 Accreditation

For a few years now there has been a recognized need 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. [37] or National Initiative for Cybersecurity Education (NICE) in the USA [27].

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 [18]. There has been a debate as to whether Cybersecurity is distinct discipline from Computer

Science [23]. 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 [1] 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. This could potentially include Cybersecurity related skills. Like the Tech Partnership the focus is upon job market requirements. Given the size of this initiative this potentially has a significant role to play however at time of writing it is not clear what that shall be.

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 [11]. 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 [10].

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

⁵Apparently <https://www.esg-global.com/research/esg-brief-2018-cybersecurity-spending-trends>.

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 and Seoul Accord (do we need to reference these). These memorandums 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 [4], [33]. 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 [29]. Clearly Cybersecurity has been and continues to be part of these 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. In parallel to the work complete by the ACM [1], 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 [20]. In 2013, an initiative was set up by (ISC)², CPHC and the Cabinet Office to examine embedding Cybersecurity into undergraduate degrees in the UK. Three workshops in 2013 and 2014 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. The BCS agreed to adopt the outputs into their accreditation criteria. This was the first time that Cybersecurity has been explicitly 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 final workshop resulted in the production of reference guidelines ("Cybersecurity Principles and Learning Outcomes") [13] that 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 [6]:

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 is 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.

3.7 What does BCS tell Universities

The agreed Cybersecurity Principles and Learning Outcome [13] were discussed with the wider education community by a roadshow lead 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 Computer Science curriculum 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 [6]. The BCS also publishes the changes that have

been made [7]. 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.

3.8 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 were required from 4 HEIs. The outcomes of these actions were as follows:

- 1) Of the 11 UG programmes involved all were approved 'At Threshold'
- 2) Of the 9 UG programmes involved, 8 were approved and 1 refused
- 3) Of the 5 UG programmes involved, all approved 'At Threshold'
- 4) 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 summation, 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.

4 CONCLUSIONS

We have the following 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 [36].
- (2) All CS courses should emphasise that informal resources should come with a "security health warning": see sections 3.3 and 3.4.

ACKNOWLEDGEMENTS

Thanks to Sally Pearce, Academic Accreditation Manager, BCS, The Chartered Institute for IT for supplying the summary information related to Accreditation.

REFERENCES

- [1] ACM/IEEE-CS Joint Task Force on Computing Curricula. 2013. *Computer Science Curricula 2013*. Technical Report. ACM Press and IEEE Computer Society Press. <https://doi.org/10.1145/2534860>
- [2] Anonymous. 2018. CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'). <https://cwe.mitre.org/data/definitions/89.html>. (2018).
- [3] Stuart Arthur, Tom Crick, and Janet Hayward. 2013. *The ICT Steering Group's Report to the Welsh Government*. Technical Report. <http://learning.gov.wales/resources/browse-all/ict-steering-groups-report/?lang=en>.
- [4] Stensaker B. and Harvey L. 2006. Old Wine in New Bottles? A Comparison of Public and Private Accreditation Schemes in Higher Education. *Higher Education Policy* 195 (2006), 65–8. <https://doi.org/10.1057/palgrave.hep.8300110>
- [5] British Airways. 2018. Customer data theft. <https://www.britishairways.com/en-gb/information/incident/data-theft/latest-information>. (2018).
- [6] British Computer Society. 2018. Guidelines on course accreditation (May 2018). <http://www.bcs.org/content/ConMediaFile/30202>. (2018).
- [7] British Computer Society. 2018. List of Changes made since 2015 v2. <https://www.bcs.org/upload/pdf/guidelines-changes-2018.pdf>. (2018).
- [8] Neil C. C. Brown, Michael Kölling, Tom Crick, Simon Peyton Jones, Simon Humphreys, and Sue Sentance. 2013. Bringing Computer Science Back Into Schools: Lessons from the UK. In *Proceedings of the 44th ACM Technical Symposium on Computer Science Education (SIGCSE 2013)*. ACM, New York, 269–274.

- [9] Neil C. C. Brown, Sue Sentence, Tom Crick, and Simon Humphreys. 2014. Restart: The Resurgence of Computer Science in UK Schools. *ACM Transactions on Computer Science Education* 14, 2 (2014), 1–22.
- [10] National Cyber Security Centre. 2018. Certification of Bachelor's and Master's Degrees in Cyber Security. (2018). <https://www.ncsc.gov.uk/content/files/protectedfiles/articlefiles/degrees-at-a-glance.pdf>
- [11] National Cyber Security Centre. 2018. NCSC degree certification. <https://www.ncsc.gov.uk/information/ncsc-degree-certification-call-new-applicants-0>. (2018).
- [12] M. Chen, F. Fischer, N. Meng, X. Wang, and J. Grossklags. 2019. How Reliable is the Crowdsourced Knowledge of Security Implementation? <https://arxiv.org/abs/1901.01327>. (2019).
- [13] CPHC, ISC2. 2015. 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).
- [14] Tom Crick and Sue Sentence. 2011. Computing At School: Stimulating Computing Education in the UK. In *Proceedings of the 11th Koli Calling International Conference on Computing Education Research*. ACM, 122–123.
- [15] F. Fischer, K. Böttinger, H. Xiao, C. Stransky, Y. Acar, M. Backes, and S. Fahl. 2017. Stack Overflow Considered Harmful? The Impact of Copy&Paste on Android Application Security. *38th IEEE Symposium on Security and Privacy (SP)* (2017), 121–136.
- [16] Mario Guimaraes, Herb Mattord, and Richard Austin. 2004. Incorporating security components into database courses. In *Proceedings of the 1st annual conference on Information security curriculum development*. ACM, 49–52.
- [17] R. Hannigan. 2019. Engineering-based industries are often not very good at cyber security. <https://events.theiet.org/cyber-ics/interview.cfm>. (2019).
- [18] M. Hentea, H.S. Dhillon, and M. Dhillon. 2006. Towards Changes in Information Security Education. *Journal of Information Technology Education: Research* 5 (2006), 221–233. <https://www.learnlib.org/p/111542/>
- [19] Matthew Horner and Thomas Hyslip. 2017. SQL Injection: The Longest Running Sequel in Programming History. *Journal of Digital Forensics, Security and Law* 12, 2 (2017), 97–107. <https://doi.org/10.15394/jdfls.2017.1475>
- [20] Alastair Irons, Nick Savage, Carsten Maple, Adrian Davies, and Lyndsay Turley. 2016. Cybersecurity in CS Degrees. *ITNow* 58 (2016), 56–57. <https://doi.org/10.1093/itnow/bww053>
- [21] Joint Committee [of Parliament] on the National Security Strategy. 2018. *Cyber Security Skills and the UK's Critical National Infrastructure: Second Report of Session 2017–19*. Technical Report HL Paper 172/ HC 706. Houses of Parliament. <https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/706/70605.htm>
- [22] Joint Task Force on Cybersecurity Education. 2017. Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity). <https://cybered.hosting.acm.org/wp/wp-content/uploads/2018/02/csec2017web.pdf>. (2017).
- [23] Andrew McGettreick. 2013. Toward effective cybersecurity education. *IEEE Security and Privacy* 11 (2013), 66–68. <https://doi.org/10.1109/MSP.2013.155>
- [24] N. Meng, S. Nagy, D. Yao, W. Zhuang, and G. Arango Argoty. 2018. Secure coding practices in java: Challenges and vulnerabilities. In *2018 IEEE/ACM 40th International Conference on Software Engineering (ICSE)*. 372–383.
- [25] Michael Page Ltd. 2018. Closing the information security skills gap. <https://www.michaelpage.co.uk/our-expertise/technology/closing-information-security-skills-gap>. (2018).
- [26] Faron Moller and Tom Crick. 2018. A University-Based Model for Supporting Computer Science Curriculum Reform. *J. Computers in Education* (2018), 1–20.
- [27] National Initiative for Cybersecurity Education (NICE). 2013. NICE Cybersecurity Workforce Framework. <https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework>. (2013).
- [28] Open Web Application Security Project (OWASP). 2017. The Ten Most Critical Web Application Security Risks. <https://www.owasp.org/index.php/Category:OWASPTopTenproject#tab=Main>. (2017).
- [29] Brooke P, Prickett T, Keogh S, and Bowers D. 2018. Becoming Professional A University Perspective. *ITNow* 60 (2018), 16–17. <https://doi.org/10.1093/itnow/bwy037>
- [30] C. Parr. 2014. Cybersecurity skills need boost in computer science degrees. <https://www.timeshighereducation.com/news/cybersecurity-skills-need-boost-in-computer-science-degrees/2016933.article>. (2014).
- [31] Allen Parrish, John Impagliazzo, Rajendra K. Raj, Henrique Santos, Muhammad Rizwan Asghar, Audun Jøsang, Teresa Pereira, Vítor J. Sá, and Eliana Stavrou. 2018. Global Perspectives on Cybersecurity Education. In *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE 2018)*. ACM, New York, NY, USA, 340–341. <https://doi.org/10.1145/3197091.3205840>
- [32] Payment Card Industry Security Standards Council (PCI SSC). 2018. Requirements and Security Assessment Procedures Version 3.2.1. https://www.pcisecuritystandards.org/documentlibrary?category=pcidss&document=pci_dss. (2018).
- [33] Mutereko S. 2017. Analysing the accreditation of engineering education in South Africa through Foucault's panopticon and governmentality lenses. *Assessment & Evaluation in Higher Education* 43 (2017), 235–247. <https://doi.org/10.1080/02602938.2017.1330395>
- [34] SPI Dynamics. 2002. White paper SQL Injection 07-31-02.doc. <https://web.archive.org/web/20030605171750/http://www.spidynamics.com:80/papers/SQLInjectionWhitePaper.pdf>. (2002).
- [35] M. Stanger and E. Martin. 2015. 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).
- [36] Cynthia Taylor and Saheel Sakharkar. 2019. DROP TABLE textbooks: An Argument for SQL Injection Coverage in Database Textbooks. In *Proceedings SIGCSE 2019*. to appear.
- [37] UK Cabinet Office. 2011. 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).
- [38] University of Bristol Cyber Security Group. 2018. The Cyber Security Body Of Knowledge: Software Security Knowledge Area Issue 1.0. <https://www.cybok.org/>. (2018).
- [39] University of Bristol Cyber Security Group. 2019. The Cyber Security Body Of Knowledge. <https://www.cybok.org/>. (2019).
- [40] T. Unruh, B. Shastri, M. Skoruppa, F. Maggi, K. Rieck, J.-P. Seifert, and F. Yamaguchi. 2017. Leveraging Flawed Tutorials for Seeding Large-Scale Web Vulnerability Discovery. <https://arxiv.org/pdf/1704.02786.pdf>. (2017).
- [41] Z. Zorz. 2019. Popular coding advice doesn't necessarily equal secure coding advice. <https://www.helpnetsecurity.com/2019/01/09/insecure-coding-advice/>. (2019).