Maintaining the Focus on Cybersecurity in UK Higher Education

### Tom Crick1, James H. Davenport2, Alastair Irons3, Sally Pearce4 and Tom Prickett5 1Swansea University

2University of Bath

3Sunderland University

4BCS, The Chartered Institute for IT

5Northumbria University

[1thomas*.*crick@swansea*.*ac*.*uk](mailto:1thomas.crick@swansea.ac.uk) [2j*.*h*.*davenport@bath*.*ac*.*uk](mailto:2j.h.davenport@bath.ac.uk) [3alastair*.*irons@sunderland*.*ac*.*uk](mailto:3alastair.irons@sunderland.ac.uk) [3sally*.*pearce@bcs*.*uk](mailto:3sally.pearce@BCS.uk) [5tom*.*prickett@northumbria*.*ac*.*uk](mailto:5tom.prickett@northumbria.ac.uk)

September 2019

Including cybersecurity in university education. We explore the progress to date.

# Introduction

Last month, a Harvard Business Review article[1] postulated that ”*Every Computer Science Degree Should Require a Course in Cybersecurity*”, provocatively reporting how cybersecurity is eating the software world and argues that systematically addressing the problem of security begins with educating software developers at scale. How could you argue with the intent of this suggestion? Alongside organisations such as the National Cyber Security Centre (NCSC), the BCS has been promoting this position for a number of years through its accreditation and policy activities and it is positive to see our concerns highlighted to a wider international audience. As our recent paper [2] argues, cybersecurity is too important to be left to specialists and hence is an essential inclusion in Computer Science, Software Engineering, and all other IT-related degree programmes.

This article explores some of the challenges raised in our paper, related to the teaching of cybersecurity in UK universities, and provides a progress report regarding BCS efforts to promote the development of cybersecurity knowledge in accredited degree programmes.

# Some Challenges

## Resources

Databases form a core part of all computer science degree programmes. From a security perspective, SQL injection is still a major concern: number one in the Open Web Application Security Project (OWASP) Top 10, and has been in the Top 10 since at least 2003. A range of common undergraduate database textbooks were analysed as part of a 2019 project [3], showing that injection attacks are generally not covered; small wonder it continues to be an issue.

Our related research from 2017 shows that Java is still the most commonly taught introductory programming language at UK universities. But many Java books generally do not cover security in depth, applied to real-world contexts. If you want to know about security you need to look at the documentation of the package/API being used, as well as a range of informal and ad hoc resources. Recent work [4] analysed 503 posting from Stack Overflow. 53% focused on Java’s Spring Framework. Of these 45% were related to authentication. One example being, by default, Spring enables protection against cross-site request forgery (CSRF). 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* ”. Needless to say, disabling security mechanisms to remove pesky errors is not a strong foundation for developing secure software and systems.

A further study [5] considered 30 popular tutorials and found six had SQL injection weaknesses, and three had Cross-Site Scripting (No.7 in OWASP’s Top Ten) weaknesses. A search on GitHub found 820 instances of these fragments, of which 117 were verified manually to be vulnerable — 80% of which were open to SQL injection attack.

## Faculty

We clearly need high quality learning and teaching in UK universities, especially in technical domains. But cybersecurity skills are in short supply, in both industry and academia. The demand for cybersecurity skills in industry makes it increasingly difficult for academia to attract academics with current knowledge, practical experience, research background and academic aspirations. As universities expand their cybersecurity provision it is not uncommon to find multiple jobs across the career path advertised at the same time.

# The Role of the BCS

Enough of the challenges ― what is being done about them? Industry, higher education, government and the relevant professional bodies have collaborated on the production of a set of guidelines which are to the benefit of the various stakeholders and wider society as discussed in a previous issue of ITNow [6]. The guidelines (“*Cybersecurity Principles and Learning Outcomes*”) published in June 2015, established a baseline of common knowledge, example learning outcome domains for cybersecurity within degree programmes and guidance on embedding the concepts.

Since 2015, the BCS have been expecting accredited degrees to be compliant with the cybersecurity guide-lines. Universities are visited on a quinquennial basis and a full cycle of accreditation visits has not yet taken place following this change in requirements. We have also observed 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 Summer 2019 term, the BCS has carried out 82 accreditation visits including five international visits (two in South Africa and one each in Brunei, Cyprus, and Ireland). The BCS identified action was required to address concerns related to cybersecurity at 23 institutions; thus, 59 institutions were already delivering cybersecurity in line with the BCS expectations.

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

Short term actions were required from nine institutions; the outcomes of these actions were as follows: (*i* ) of the eleven UG programmes involved all were approved ‘*At Threshold* ’; (*ii* ) of the nine UG programmes involved, eight were approved and one refused; (*iii* ) of the five UG programmes involved,

all were approved ‘*At Threshold* ’; and (*iv* ) of the three UG programmes involved, all were refused; and (*v* ) a further five which at the time of writing the outcome is not known

Good practice was identified at three universities by the commendation:

“*The second-year project provides an opportunity for exploring security aspects in depth with an industrial use case.*”

“*Hacktivity and related learning and teaching approaches*”

“*Cyber Security Centre which permeates both the course and supports external links and opportunities for students.*”

# Looking Ahead

The BCS is improving the cybersecurity capacity in the UK by enhancing the education experience of the students on BCS accredited degree programmes. If you want to be reassured that the graduates you recruit have some cybersecurity knowledge, then seek a BCS accredited degree. There are challenges ahead in terms of enhancing the resources upon which the degree provision depends and developing the cybersecurity capacity within universities.

As a final rhetorical point, is it sufficient to leave to cybersecurity to Computer Scientist? Should it be solely the preserve of those who work with Tech? Or should it be everyone’s responsibility? We hope this is a conversation that will begin shortly.

# References

[1] J. Cable *Every Computer Science Degree Should Require a Course in Cybersecurity, Harvard Business Review* 27th August 2019

[2] T. Crick, J. Davenport, A. Irons , T.. *A UK Case Study on Cybersecurity Education and Accreditation.* In Proc. of 2019 *IEEE Frontiers in Education Conf*. <https://arxiv.org/abs/1906.09584>

[3] C. Taylor and S. Sakharkar. ’*;DROP TABLE textbooks;–* An Argument for SQL Injection Coverage in Database Textbooks. In *Proc. of SIGCSE 2019*, pages 191–197, 2019.

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

[5] 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.

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