Leslie F. Sikos
Paul Haskell-Dowland *Editors*

Cybersecurity Teaching in Higher Education

Springer

Cybersecurity Teaching in Higher Education

Leslie F. Sikos • Paul Haskell-Dowland
Editors

Cybersecurity Teaching in Higher Education

Springer

Editors
Leslie F. Sikos
School of Science
Edith Cowan University
Joondalup, WA, Australia

Paul Haskell-Dowland
School of Science
Edith Cowan University
Joondalup, WA, Australia

ISBN 978-3-031-24215-1 ISBN 978-3-031-24216-8 (eBook)
https://doi.org/10.1007/978-3-031-24216-8

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

With the cost of cybersecurity-related incidents estimated to be more than $1 trillion worldwide, it is perhaps no surprise that cybersecurity has become a global priority. This is clearly visible when we look at popular media and the rise of cybersecurity as a topic of public debate. Incidents often include the exposure of personal data; deceiving, highly personalized messages and chat conversations; and an ever-growing variety of cyberattacks not detectable by traditional protection mechanisms.

While the difficulties of providing secure platforms, products, and services are well known, the solutions are still challenging those in academia, industry, and government as there is a significant mismatch in supply and demand of skilled professionals (the "cyber-army").

Although we can argue over the size and nature of the so-called "skills shortage" (with many acknowledging that it is an *experience* as much as a *skills* shortage), the growing demand for trained cybersecurity professionals seems to be expanding the gap with every passing day.

In most developed countries, the demand for cybersecurity practitioners is far greater than the pipeline of students electing to study in aligned courses. The situation is even more dire in developing countries where there is often no pathway to develop the skills in-country, thus often being entirely dependent on the importation of cybersecurity capabilities at a time of global demand.

There are many facets to these problems, but the key is to enable, endorse, encourage, and invest in cybersecurity at all levels. Cybersecurity awareness needs to begin at the earliest level of education and be reinforced throughout curriculum and lifelong learning (from cradle to grave). This awareness and generalized cybersecurity capability then needs to be supplemented by highly educated, trained, and experienced cybersecurity professionals, and this is why cybersecurity has been taught at the tertiary level globally for years, with an increasing number of universities adding it to their course offerings. However, teaching cybersecurity in higher education has unique challenges due to the evolving nature of the field as well as the diverse range and high complexity of the computing systems we have today. These include, but are not limited to, how to generate authentic datasets for case studies without illegal activities and including sensitive corporate or personal data; gaining access to industry-leading solutions in a lab setting; and teaching information security teamwork for online students.

This book is a collection of approaches and practices to address some of the aforementioned issues.

Chapter 1 discusses the main challenges and arising opportunities of teaching cybersecurity at universities. In particular, it details how to develop cybersecurity competencies through university courses, illustrated with the approaches of various universities, covering the applied modules, effectiveness, practices shared by multiple universities in the UK, and future actions.

Chapter 2 describes the application of the Delphi method for collecting and prioritizing requirements for international Master's programs in information security management. The authors engaged with industry practitioners ranging from information security consultants to CISOs.

Chapter 3 demonstrates how to realize scenario-based learning for cybersecurity in tertiary education. To develop a curriculum based on this, the relevant topics have been shortlisted, the context identified, and scenarios created. This chapter also describes the challenges of facilitating sessions where students are assigned to teams to discuss a scenario.

Chapter 4 details the challenges of teamwork in cybersecurity courses in higher education, frameworks used in this field, and practices for supporting the development of teamwork skills. It also describes how to develop project management and creative problem solving skills in cybersecurity, and support student engagement and satisfaction.

Chapter 5 discusses quality criteria for massive open online courses in cybersecurity, how to evaluate compliance, and what are the certification criteria.

Chapter 6 discusses the main considerations and technology-advanced learning environments suitable for teaching digital forensics both for in-class and online university students. It also lists the main technological, legal, administrative, and pedagogical challenges and how to overcome them.

Joondalup, WA, Australia
April 2023

Leslie F. Sikos
Paul Haskell-Dowland

Contents

Challenges and Opportunities of Teaching Cybersecurity in UK University Computing Programmes 1
Tom Prickett, Longzhi Yang, Alastair Irons, Keith Miller, Phil Brooke, Tom Crick, Alan Hayes, James H. Davenport, Rosanne English, Joseph Maguire, Kamal Bechkoum, and Andrew Jones

Using the Delphi Method to Elicit Requirements for an International Master's Program in Information Security Management 37
Fredrik Karlsson, Karin Hedström, and Ella Kolkowska

Designing and Developing a Scenario-Based Curriculum for Cyber Education in HE 59
Rosanne English

Enabling Teamwork in Cybersecurity Courses 79
Joanne L. Hall and Asha Rao

Towards a Light-Weight Certification Scheme for Cybersecurity MOOCs 103
Matthias Beckerle, Argyro Chatzopoulou, and Simone Fischer-Hübner

Learning Environments for Digital Forensics Teaching in Higher Education 127
Leslie F. Sikos

About the Editors

Dr. Leslie F. Sikos is a computer scientist specializing in artificial intelligence and data science, with a focus on cybersecurity applications. He holds two Ph.D. degrees and 20+ industry certificates. He is an active member of the research community as an author, editor, reviewer, conference organizer, and speaker; a senior member of the IEEE, and a certified professional of the Australian Computer Society. Dr. Sikos published more than 20 books, including textbooks, monographs, and edited volumes.

Holding a Master of Education in IT, and having taught at four universities on two continents, he has a strong pedagogical background and teaching expertise using active learning theories, from social constructivism and problem-based learning to narrative-based teaching, as well as the BSCS 5E instructional model, covering in-class/on-campus, hybrid (blended), online, and accelerated online delivery modes for undergraduate and postgraduate students. This is complemented by experience in cybersecurity unit and course coordination, Ph.D. supervisions in cybersecurity, and being a theme lead of a research project proposing changes to the Government of Western Australia on incorporating new cybersecurity components in school curricula (https://www.lesliesikos.com).

Prof. Paul Haskell-Dowland is the Associate Dean for Computing and Security in the School of Science at Edith Cowan University, Perth, Australia.

Paul has maintained a significant interest in cybersecurity education with leadership roles in higher education institutions. Paul has led teams delivering cybersecurity education at undergraduate and postgraduate level including research programs through to Ph.D. Paul is the ACS/Australian Country Member Representative and Chair of the International Federation for Information Processing (IFIP) Technical Committee 11; a member of the ACS Cyber Security Committee; a Fellow of the Australian Information Security Association; and a Fellow of UK HE Advance (FHEA)—all with a focus on cybersecurity education, training, and awareness.

In addition to his academic leadership role, Paul has delivered keynotes, invited presentations, workshops, professional development/training, and seminars across the world. He has appeared on local, national, and international media (newspaper, radio, and TV) commenting on current cyber-issues with a global audience reach of more than 2.5 billion people. His contributions through articles published in *The Conversation* have reached over 3 million readers—joining the top-50 authors in Australia/New Zealand. Paul has more than 20 years of experience in cybersecurity research and education in both the UK and Australia.

Challenges and Opportunities of Teaching Cybersecurity in UK University Computing Programmes

Tom Prickett, Longzhi Yang, Alastair Irons, Keith Miller, Phil Brooke, Tom Crick, Alan Hayes, James H. Davenport, Rosanne English, Joseph Maguire, Kamal Bechkoum, and Andrew Jones

1 Introduction

Cybersecurity is now an integral part of digital technologies, from both a technical and socio-technical perspective; indeed, it is a increasingly explicit feature of our world: societally, culturally and certainly economically. Given that cyber attack can happen in many different ways over all sorts of computing devices and their connected hosts or peripherals, the education of cybersecurity is seen as an indispensable part of all computing degree programmes by increasingly more employers and higher education providers [26]. This growing consensus has been well captured by the professional, statutory and regulatory bodies (PSRBs) in the UK and internationally, and articulated in the curricula recommendations

T. Prickett · L. Yang (✉)
Northumbria University, Newcastle upon Tyne, UK
e-mail: tom.prickett@northumbria.ac.uk; longzhi.yang@northumbria.ac.uk

A. Irons
University of Abertay Dundee, Dundee, UK
e-mail: a.irons@abertay.ac.uk

K. Miller
Manchester Metropolitan University, Manchester, UK
e-mail: k.miller@mmu.ac.uk

P. Brooke
Green Pike Ltd, Guisborough, UK

Northumbria University, Newcastle upon Tyne, UK
e-mail: phil@green-pike.co.uk

T. Crick
Swansea University, Swansea, UK
e-mail: thomas.crick@swansea.ac.uk

L. F. Sikos, P. Haskell-Dowland (eds.), *Cybersecurity Teaching in Higher Education*, https://doi.org/10.1007/978-3-031-24216-8_1

by the Association of Computing Machinery (ACM)/Institute of Electrical and Electronics Engineers (IEEE), the Quality Assurance Agency (QAA) Benchmark Statement, the accreditation mapping criteria by British Computer Society (BCS), The Chartered Institute for IT and the Cyber Security Body of Knowledge (CyBOK) by the National Cyber Security Centre (NCSC) as a promotion from the UK Government, amongst others. This is in the wider context of major and ongoing digital skills [19, 52, 53] and computer science curriculum reform [4, 5, 35, 45] in the UK and internationally, alongside a renewed focus on what should be taught as part of technical degree programmes [36, 47, 56], and how it should be taught [7, 11, 18, 20].

This chapter focuses upon the growth of cybersecurity education and the challenges and opportunities it presents for mainstream higher education computing programme provision. It contextualises the growth of cybersecurity, as a taught entity, through an analysis of the development and establishment of various professional and accreditation criteria regarding the teaching of cybersecurity in computing degree programmes. Accreditation of degree programmes by PSRBs is a common practice, but it is not universally popular. It has been variously criticised as unnecessarily bureaucratic, constraining innovation (and academic freedom) [25], revenue streams for accrediting bodies rather than of value in their own right [31] and even colonial in nature [37]. However equally the value of accreditation schemes particularly in terms of a globally mobile workforce must also be highlighted [9]. In the Computing discipline in the UK, bodies have been working to encourage and improve the standard of security education embedded in computing degree programmes to help promote curricula relevance in this area [8, 12, 13].

This chapter also reviews how the sector has positioned itself against these emerging criteria. In particular, the distinction is made between specialist programmes in cybersecurity and mainstream generalist computer science provision that addresses cybersecurity as one of a number of emerging technologies that encompass the core body of knowledge that constitutes the subject area of com-

A. Hayes · J. H. Davenport
University of Bath, Bath, UK
e-mail: ah347@bath.ac.uk; masjhd@bath.ac.uk

R. English
University of Strathclyde, Glasgow, UK
e-mail: rosanne.english@strath.ac.uk

J. Maguire
University of Glasgow, Glasgow, UK
e-mail: joseph.maguire@glasgow.ac.uk

K. Bechkoum
University of Gloucestershire, Cheltenham, UK
e-mail: kbechkoum@glos.ac.uk

A. Jones
The Cyber Scheme, Cheltenham, UK
e-mail: Andrew.jones@thecyberscheme.org

puting. A number of current case studies are presented from a range of higher education institutions (HEIs) as a means of sharing a sample of current practice. An analysis of these case studies is presented by identifying both differing and similar practices across the samples. From this, the relative merits are summarised in developing bespoke cybersecurity units versus integrating cybersecurity issues across a number of units and levels within the curriculum. Finally, this wider work has been conducted through the ongoing lens and impact of the COVID-19 pandemic on education globally, across all settings and contexts [6, 26, 57, 58], but with distinct impacts and emerging challenges for computer science as an academic discipline [14, 15, 17, 46].

The reminder of this chapter is organised as follows: Sect. 2 reviews the policy of teaching cybersecurity in the UK; Sect. 3 reports several case studies performed in representative UK HEIs; Sect. 4 summarises the case studies and makes recommendations; and Sect. 5 concludes the chapter.

2 Policy and Teaching Cybersecurity in the UK

The need to develop a pipeline for study of cybersecurity has been recognised for over 10 years in the UK, with the National Cyber Security Strategy 2011–2016 noting the need to build skills to underpin all cybersecurity objectives [54]. The National Cyber Security Strategy 2016–2021 further identified the need to address the systemic problem of attracting young people into the cybersecurity profession [55]. The UK Government's Department of Digital, Culture, Media and Sport (DCMS, which is where "digital", AI and societal-facing technology activities tend to sit) sponsored annual Cyber Discovery programme targeting 13–18 year old arose from 2016 to 2021 strategy. To facilitate learning there were intrinsically-motivating tasks such as problem-solving challenges, webinar activities, lab practicals, often in a gamified context. The first part of the programme consisted of an assessment phase designed to identify students with an aptitude for cybersecurity. Those who demonstrated this were able to progress to elite Discovery Camps. The evaluation of the Cyber Discovery programme indicated success in student engagement, with participation targets greatly exceeded [22]. Furthermore, it was successful in meeting targets for engaging female and ethnic minority students. However, the evaluation of Cyber Discovery found no evidence that the programme increased interest in cybersecurity more widely as a study subject or as a career.

CyberFirst is a related initiative for students aged 13–18 to increase interest in the study of cybersecurity. The programme was introduced in 2016 and sponsored by the UK's National Cyber Security Centre (NCSC). It comprises a progressive set of courses that supports pathways into university courses and Degree Apprenticeships (DAs), and offers financial support through bursaries. CyberFirst incorporates a girls-only competition that seeks to address the gender imbalance. An independent evaluation of CyberFirst in 2021 [21] found that those who took part had an increased interest in cybersecurity, and those participated in summer courses were more likely to apply for a cybersecurity course.

Whilst both Cyber Discovery and CyberFirst have increased awareness in cybersecurity, neither programme claims to have improved HE recruitment amongst attendees but this may in part be due to the fact they are still at a relatively early stage of their education and are likely to have many career options. However, both programmes have had success in attracting students from under-represented groups (i.e. female, ethnic minority and low participation neighbourhoods). Further, there is evidence of a community of practice developing between schools, industry experts and alumni from the programmes, which can be built upon in the future, to develop further engagement. The continuation of government funding received by both programmes indicates their value in promoting cybersecurity to 13–18 year old, but the evaluation outcomes suggest further work is needed to build the pipeline into cybersecurity study and that schools, employers and HEIs will need to work together to build capacity to meet demand.

DAs were introduced in 2015 by the UK government as a way of addressing industry needs, targeting areas of skills shortages. DAs bring together academic rigour from higher education and practical skills development from vocational education. They can be studied at level 6 (final year of undergraduate degree) or level 7 (master's degree). The students must be employed and sponsored by a company, and they spend at least 20% of their time studying for the award. Companies can use the apprenticeship levy, a tax that would normally be paid to the Government, to pay students' tuition fees. Students take part in work-based learning, i.e. some coursework and exercises is linked to work that are carried out in their normal employment. The curriculum framework for each DAs is designed by employers, universities, and colleges to produce graduates well-equipped for their disciplines. The benefits for students are that they learn in context in a supportive work environment and are paid whilst they study. The benefits for employers are that student learning is geared towards the needs of their businesses and it is reported retention rates of graduates is high. The BSc Digital and Technology Solutions (DTS) DA is aligned to Computer Science (CS) curriculum and currently there are 46 providers in the UK.

But this is not enough. National Cyber Security Strategy was set up aiming to fully address this. For the long run, Cybersecurity is a fundamental skill expected from every computer science graduate. In the UK, accreditation schemes and curricula guidelines have emerged to help promote this.

2.1 National Cyber Security Centre (NCSC) Certification

The National Cyber Security Centre (NCSC), a part of the UK Government Communications Headquarters (GCHQ), has established a certification programme for taught degrees that either specialise in cybersecurity or cover a significant cybersecurity component. The programme started in 2014 and was originally open to postgraduate courses only, but is now available for both undergraduate and postgraduate courses, including DAs. At the time of writing, 49 degrees were certified from 34 UK universities [39]. Of these degrees, 35 were at postgraduate level, 12 at undergraduate level and 2 DAs.

2.1.1 The Cyber Security Body of Knowledge (CyBOK)

A key requirement for the certification is for the degree learning outcomes to be mapped against the Cyber Security Body of Knowledge (CyBOK) [44]. Led by the University of Bristol in collaboration with a number of other universities and experts from industry. The aim of CyBOK is to provide a comprehensive body of knowledge based on an extensive literature search as well as an in-depth consultation involving key stakeholders both in the UK and internationally. This work culminated in a body of knowledge comprising 21 Knowledge Areas (KAs) spanning five categories.

2.1.2 The Application Process

Each year the NCSC issues a call for applications. HEIs can submit an application for a Full Certification of the degree or a Provisional one. The Full Certification is for degrees that have been running long enough for students' assessment work to be available for scrutiny, including dissertations. Applications for Provisional Certification must confirm that the degree has already started or will start by the next academic year. Each submission must be accompanied with a letter of support from senior management (usually the Vice Chancellor) to confirm that the senior management of the institution is fully supportive of the application. The application must demonstrate how the institution meets the certification criteria described below.

2.1.3 Certification Assessment Criteria

Assessment criteria fall under six main categories, namely:

- Description of the applicant (team knowledge and expertise, facilities and recent investments, external linkages, review and update process).
- High level description of the degree (key characteristics, delivery, aims).
- The taught component of the degree (overall distribution of credits, number of credits that can be mapped against Computer Science and CyBOK KAs, Module descriptors' consistency with KAs covered, addressing professional and knowledge skills).
- Individual projects and dissertations (level and credit value, timeline, governance, guidance to students, identification and selection of project topics, allocation of students to supervisors, legal and ethical issues, monitoring of students' progress,