

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>

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2023

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

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 an 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

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 remainder 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,

detecting and dealing with plagiarism, the marking/grading process). For Full Certification, applications must also provide a list of dissertations undertaken by students demonstrating that the topics are within the CyBOK KAs).

- Student numbers and grades Achieved, which applies only to Full Certification.

2.1.4 A Rigorous Process of Certification

Independent expert assessors are appointed from both academia and industry. Each assessor is given three to five applications to assess, with each application being assessed by three assessors. Assessors grade each criterion (or sub-criterion) as 'Achieved', 'Not Achieved', 'Unclear' or 'Not Applicable'. Where needed, assessors can provide brief comments. Once input is collated from all assessors, a panel is convened whereby individual applications are reviewed in light of the feedback received from the three related assessors. The panel discussion tends to focus only on areas where there is not consensus between the assessors, with a view to reach to an assessment outcome that is agreed by all. The final outcome is then communicated to the applicant, which can be 'Achieved', 'Further Information Needed', or 'Not Achieved' and a resubmission would be required. In the latter two cases, a more detailed feedback is provided to the applicant institution via email or during a meeting if required.

2.1.5 The Merits of the Certification

The Certification is increasingly regarded as a strong indicator of quality by students and employers alike. For prospective students, a NCSC-certified degree helps make better informed choices about the quality of courses available. For employers the certification provides a level of assurance that students will enjoy a high-quality learning experience that endows them with the much valued industry skills. For universities and higher education providers, the certification helps to attract high quality students and high calibre staff, from around the globe. The certification is also a route for the HEI to achieve the status of an Academic Centre of Excellence in Cyber Security Education, ACE-CSE.

2.1.6 NCSC Review and Survey

The NCSC conduct an annual review of cybersecurity [38] and an annual cybersecurity breaches survey [23]. The annual review is an authoritative evaluation of key developments and highlights in cybersecurity that impact the UK. The cybersecurity breaches survey presents an annual snapshot of the key threats and their impacts on businesses. The survey shows the distribution of attacks by category and the financial effect. Together the reports provide an evidence base for where companies

should focus resources to best protect themselves and for where universities should develop their curriculum.

2.2 BCS Degree Accreditation

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. This resulted that all accredited universities being compliant by 2020 (due to the 5-year cycle).

A series of development workshops were organised by the BCS, Council of Professors and Heads of Computing (CPHC), and International Information System Security Certification Consortium ((ISC)²) throughout 2014 and 2015. One of the key outcomes from the workshops was the opportunity to embed cybersecurity in the curriculum. Another outcome was the BCS Academic Accreditation criteria were updated to include reference to cybersecurity as an indication of the importance of the need for cybersecurity [12].

A review [13, 16] was undertaken by the Academic Accreditation Committee of the BCS in 2015 and cybersecurity was embedded as one of the criteria to be reviewed (where taught and assessed in the curriculum) as part of the Chartered IT Professional (CITP) and Chartered Engineers (CEng) criteria for accreditation of computing and computer science courses in universities. The specific criteria to measure cybersecurity are summarised in Table 1.

As part of the collaborative work between BCS, CPHC and (ISC)² a specific curriculum is expected including coverage [27] of:

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

Table 1 BCS cybersecurity criteria

Location	Content
[3, p23]	Requirements for Accreditation of Honours Programmes (and generalist masters programmes) for CITP
2.1.5	Knowledge and understanding of Information security issues in relation to the design, development, and the use of information systems
2.1.7	Knowledge and understanding of methods, techniques and tools for information modelling, management, and security
[3, p28]	Requirements for Accreditation of Honours Programmes for CEng, the Accreditation of Higher Education Programmes (AHEP version 4)
C10	Adopt a holistic and proportionate approach to the mitigation of security risks

This syllabus has also been adopted by the Institution of Engineering and Technology (IET). This is additional to the general expectations of CEng as required by the Engineering Council [24].

2.3 *Quality Assurance Agency (QAA) Benchmark Statements*

The Quality Assurance Agency (QAA) defines the Academic Infrastructure as being a set of nationally agreed reference points which give all institutions a shared starting point for setting, describing and assuring the quality and standards of their higher education courses. They work closely with the UK higher education sector to develop these reference points. One such reference point is the Subject Benchmark Statements (SBSs). SBSs set out expectations of standards of degrees in a range of subject areas. They describe what gives a discipline its coherence and identity and define what can be expected of a graduate in terms of the techniques and skills needed to develop an understanding in the subject. The majority of UK universities will have used and referenced their respective SBS in the development of their programmes and curriculum.

The development and emergence of cybersecurity can be tracked through its prominence on the evolution and release of the QAA SBSs for Computing. The 2007 QAA SBSs for computing does not explicitly reference cybersecurity in either the main core text or the Body of Knowledge contained in its appendix. In the 2016 release, cybersecurity is only mentioned twice, as a stream within the subject areas of both Software Engineering and Information Technology. Software Engineering treats cybersecurity in the context of information security and safety critical systems whereas Information Technology views cybersecurity through the lens of risk and service management of IT systems.

The 2019 mid-term review of the SBSs can be seen to mark the growing importance of cybersecurity. There is an explicit reference to ACM (2017) Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. Cybersecurity features prominently in the 2022 release of the SBSs [43]. It is recognised both as an emerging area for graduate employment and a growing feature in the design of computing degrees. Cybersecurity is also recognised as a distinct discipline area of the broad subject field of computing and computer science.

2.4 *ACM Curricula*

The Association of Computing Machinery (ACM) has had cybersecurity in the curriculum since the formation of 2013 ACM/IEEE-CS Joint Task Force as reported in the Information Assurance and Security (IAS), but it is not an accrediting body. The Accreditation Board for Engineering and Technology (ABET) is an accrediting body which requires IAS with effect from the 2019–2020 academic year (self-study

reports due 1 July 2019). This is detailed in Table 3 in [40] as “the computing topics must include: principles and practices for secure computing. . .”. This means that all accredited universities should be compliant by 2025, due to the 6-year accreditation cycle.

An ACM working group [42], established in 2018 as part of the Innovation and Technology in Computer Science Education (ITiCSE) conference series, has been capturing global perspectives on cybersecurity education. The main focus of the working group’s report is towards defining security as a meta discipline as such the findings will be of more utility to specialist cybersecurity related programmes rather than more mainstream offerings.

ACM 2020 curricula, recognised cybersecurity as a discipline within its own right and provide guidance for such degree offerings. These curricula recommendations indicate “security permeates the entire space of computing” [1, p31] and hence recommend its inclusion within all discipline areas of computing; and “some areas (e.g. cybersecurity) even have their own formal guidelines” [1, p31]. The curricula guidance is provided by certain type of degrees including computer engineering cybersecurity, computer science, information systems, information technology and data science. In the UK jurisdiction computing degree programmes do not always naturally fit into each of these distinct areas with combinations between the sub-discipline areas being common i.e. a computer science degree with a security focus. The adopted approach makes the curriculum guidelines useful within curricula design, however, a degree programme would not necessarily directly follow the recommendations from one sub-discipline.

The QAA Benchmark (see Sect. 2.3) cross references the ACM curriculum guidelines, again highlighting their utility but they remain focused upon degree provision in the USA so not all aspects are necessarily directly portable to the UK jurisdiction.

2.5 Industrial View

Industrial employers, referring to both private and public sectors, require generalist computing graduates. These graduates are employed across the full breadth of activity. Some may be producing computer-based products for end-users, such as appliances (white goods, televisions), Apps (delivered via Google Play or Apple Store), web pages, e-commerce services and other traditional computer software. Others will be providing computing services or support to organisations for the delivery of their aims. This could be maintaining human resource (HR) and payroll systems, general infrastructure, virtualised platforms and domain-specific systems. The increased use of cloud providers may have reduced some of the demand for local server systems but still requires IT management and administration. Large organisations may have multiple layers of help- and service desks. The staff in all of these areas are unlikely to be specialist information security professionals, but they

necessarily require some understanding of the issues involved with cybersecurity. Some examples include:

- Recognising that calls to a service desk, or low-priority notifications, may be the first warning that a cyber attack is underway: the first notification of the SolarWinds attack was a notification of multi-factor authentication (MFA) enrolment [2] which an alert help desk operation followed upon.
- Designing a software product and understanding where specialist support is required from cybersecurity and data protection professionals is needed.
- Deploying internal services (email, instant messaging, file servers) securely and reliably. None of these require cyber specialists, especially when there is a shortage of potential staff. Indeed, some of these roles require people with specialisms in other areas. Regardless they need a baseline level of understanding of information security so they can interoperate with and escalate issues to cyber specialist staff.
- Good coverage of the five themes as jointly recommended by BCS, CPHC and (ISC)² broadly addresses this for most computing students [27].

3 Case Studies

This section provides seven cases studies designed to be illustrative of the emergent practice related to embedding security in general computing degree provision across the UK. A range of types of HEI are represented, including research intensive and more teaching focused universities. The approaches each university has adopted is explored, including the rationale for the approach, innovative features, together with a brief evaluation and intended future developments. A structured approach is adopted broadly around the questions: What is it? (i.e. The Approach); Where does it fit? (i.e. Applied Modules/Programmes); Does it work? (i.e. Effects and Effectiveness); Who else has done this? (Similar Practice in Other HEIs); What will you do next? (i.e. Future Actions); and Why are you telling us this? (i.e. Final Notes). The case studies are further analysed in the subsequent section in which the impact of related accrediting bodies is explored, with the support of a summary of the adopted approaches and outcomes.

3.1 *Northumbria University*

3.1.1 **The Approach**

One approach to embedding cybersecurity within the curricula is to treat cybersecurity as a cross curricula concern and include related aspects as relevant in other curricula areas. In other words, programming module address secure programming;

threats and attacks are addressed in a technology specific way with for example SQL Injection being addressed in web/cloud related areas of the curricula and so on. Treating security as a cross-curricula concern, also means embedding security as small tasks across the programme of study (i.e. security is assessed by tasks within broader assessments). The BCS Guidelines (Sect. 2.2 of this chapter) were employed to help define the curricula content.

3.1.2 Applied Modules/Programme

This approach has been adopted for a mainstream undergraduate CS programme within one modern teaching and research focused UK university, for a large undergraduate CS programme which regularly recruits over 200 students. Crick et al. discussed the implementation in more details [10].

3.1.3 Effects and Effectiveness

On the positive side, security becomes integral of all aspects of the discipline. This highlights security is always a concern that needs to be addressed and addressing it is part of normal practice. Less positively, security when assessed is a small component of a wider assessment, so that some learners could perceive it as peripheral and not as important as other curricula issues. Also, less positively, embedding across the curricula creates a management overhead. Faculty need to be constantly reminded of the need to ensure its inclusion, or there is a tendency for the syllabus to drift and the security content to be replaced with other items the delivering faculty find more interesting (and possibly closer to their personal research interests).

To help address some of the less positive consequences, a Visiting Industrial Professor was appointed, to emphasise to the learners the practical importance of security in the commercial environment. The Visiting Industrial Professor is a senior industrialist specialising in cybersecurity who works for the related department for 12 days of the academic year. The contributions of the Visiting Industrial Professor are varied: they advise upon context; they design, develop, and deliver classes; they mentor learners with interests in security careers and provide developmental support to academic faculty.

Within any cohort of learners there are very engaged learners and learners whose engagement is more strategic [30], with such learners tending to a solely focus upon assessment tasks. Engagement with the Visiting Industrial Professor is quite varied with engaged learners making considerable use of the available support and commenting positively upon its inclusion within the curricula. Discouragingly, for the more strategic learners in the cohort, there is a tendency to see this enhancement activity as an optional extra which does not directly support the assessment activities they are focused upon. This is a misconception on behalf of learners as the guidance does extend to the assessed work.

3.1.4 Similar Practice in Other HEIs

This approach has been adopted for the mainstream undergraduate CS programmes within several UK universities, often with large cohorts. It has also been adopted in disciplines allied to computer science such as software engineering (for example games development), information technology and information systems. Computer engineering degrees commonly have been addressing cybersecurity in a technical sense for some time. The approach taken within such programmes is commonly to include one or more course which address security directly or as a significant concern with examples such as network security, ethical hacking / offensive security, etc. Within Cybersecurity programmes coverage of security is ubiquitous.

3.1.5 Future Actions

Whilst the inclusion of cybersecurity as a cross discipline concern was a step forward in terms of coverage, there remain some outstanding issues with the approach. The next step is to supplement the cross curricula coverage by the inclusion of a course in the programme which has security as its principal focus. The intent is to maintain coverage in a cross curricula fashion for the most significant areas, for example technology related threats and attacks and secure programming. However other aspects of security are planned to be delivered mainly in the new course.

3.1.6 Final Notes

To understand the recommendations that we propose, it is important to understand the explorations we have completed into alternative approaches. Next, we shall consider cybersecurity within one course, this will then be followed by initiatives to deliver cybersecurity within one module and supplementing that by cross curricula inclusion.

3.2 *Sunderland University*

3.2.1 The Approach

The University of Sunderland participated in the development workshops organised by the CPHC and (ISC)² throughout 2014 and 2015 [13, 27], and one of the key outcomes from the workshops was the opportunity to embed cybersecurity in the curriculum. In parallel with the CPHC and (ISC)² workshops, feedback from the Department's Industrial Advisory Board indicated that there was a skills gap in CS

graduates with cybersecurity knowledge. The final piece in the jigsaw was when the BCS published the revised accreditation guidelines (see Sect. 2.2 of this chapter) that included a reference to newly published Cyber Security Principles and Learning Outcomes for Undergraduate Computing Science in the United Kingdom [27]. The decision to integrate cybersecurity topics into the curriculum at the University of Sunderland was timely in that it coincided with the quinquennial periodic review of undergraduate programmes in early 2015.

3.2.2 The Applied Modules/Programmes

This gave colleagues the opportunity to discuss and debate the opportunities and issues associated with enhancing the coverage of cybersecurity in the curriculum. As part of the review colleagues made use of the principles and learning outcomes that were identified in the CPHC/(ISC)² workshops and tried to embed across a range of computing disciplines and subject areas. As a programme team we utilised the principles and learning outcomes in a series of steps:

- identified the coverage of cybersecurity already in place (tended to be in networking and database modules);
- identified new areas (computing fundamentals module in year 1, software development project in year 2, programming modules throughout the CS programme);
- enhanced coverage in non-security modules—particularly programming, database modules, networking modules, web modules and mobile development;
- added a new specialist cybersecurity module in final year (core to CS, Computer Forensics, Network Computing and an option on other undergraduate programmes).

Cybersecurity as embedded in the Sunderland CS programme is summarised as follows:

Stage 1

K5—Knowledge of the expectations of the key cybersecurity properties of confidentiality, integrity and availability.

S6—Employ conceptual tools across all aspects of the systems life cycle, including: requirements analysis, specification, implementation, *security design*, testing, documentation and maintenance.

Stage 2

K6—Understanding of the industrial, *security*, professional, legal and ethical issues associated with computer-based systems.

K8—Knowledge of a range of specialist computing techniques and how they may subsequently be applied to solve real-world problems within an application domain *in a secure and trustworthy environment*.

Stage 3

K12—An in-depth understanding of the state of the art in selected specialist area(s) of CS e.g. Artificial Intelligence, *Cybersecurity*, Object Oriented software development, Databases.

In addition, there is an expectation that cybersecurity is covered as one of the fundamental topics in Stage 3 and is embedded in the generic learning outcomes and illustrated by students in the following programme learning outcomes:

S9 Undertake independent research in order to identify appropriate methods, tools, and techniques to address complex problems

S10 Design, build and evaluate complex software artefacts using a wide range of development methods, languages and platforms

S11 Learn, critically appraise and evaluate both new concepts in technology and own skills development in preparation for the life-long challenge of working in a continually changing environment

3.2.3 Effects and Effectiveness

Integrating cybersecurity into the curriculum is one of the components that has seen an increase in graduate employability from less than 70% in 2014 to greater than 90% from 2018 onwards. The student engagement with cybersecurity on the undergraduate programmes was one of the drivers for the MSc Cybersecurity programme which was first run in 2017. Subsequent programme developments have seen MSc Computer Science with Cybersecurity (online) and a cybersecurity strand included in the University of Sunderland's MBA programme.

There was investment in a new cybersecurity/digital forensics lab in 2017 and two specialist cybersecurity lecturing posts were approved and appointed to in 2018.

3.2.4 Similar Practice in Other HEIs

Other universities have included cybersecurity as part of their undergraduate curriculum—often because of the BCS requirement for cybersecurity coverage. Not everyone has utilised the same approach as Sunderland—embedding across a series of modules, then having a specialist module in final year.

3.2.5 Future Actions

Moving forward we will continue to have cybersecurity embedded in the CS programme and continue to enhance the facilities for teaching and learning for cybersecurity. The team are also working closely with local and national employers to have industrial input to the cybersecurity strand and to identify placement (often difficult because of clearance requirements) opportunities, internships and projects.

3.2.6 Final Notes

The approach adopted by Sunderland is one of the ways to embed cybersecurity. The approach has proved popular with students and with employers.

3.3 Manchester Metropolitan University

3.3.1 The Approach

MMU was part of the first group of universities to DAs in computing when the BSc (Hons) Digital Technology Solutions (DTS) degree was launched in 2016. A DA is a higher education course that combines work with part-time study. The DTS DA programme was developed in partnership with national industries and is accredited by the BCS and Tech Partnership Gold. It is delivered over 4 years and makes use of a blend of day release, block teaching and workplace learning. At MMU, there are four DTS pathways, including Software Engineering (two pathways one of which is a specialist mainframe route), Cyber Security, Data Analytics and IT Consultancy. All students must be employed in a relevant role with commitment from their employer to support university study. Students across all pathways take the Computer Fundamentals which covers aspects of cybersecurity such as essentials of database and network security. In addition, all students are required to consider the security implications of their product in their final year project. Software Engineering and Cyber Security pathways have additional cyber security content.

3.3.2 Applied Modules/Programmes

The DTS DA sits alongside mainstream UG CS provision at MMU. It enables students to earn a salary while studying which is a significant financial incentive. Across all MMU apprenticeships, 36% comes from the most deprived areas (Index of Multiple Deprivation (IMD) [34] 1–4), hence the DTS course can be viewed as a vehicle for social mobility. More significantly, in terms of attainment, students work in an environment that is supportive to their study with easy access to expert mentors. The nature of DAs with embedded work-based learning, enable students to apply cyber security concepts to platforms and development environments used in their jobs which promote understanding.

3.3.3 Effects and Effectiveness

Outcomes from the DTS DAs have been very high. The first cohort of DTS apprentices had an average salary of GBP39,000, almost 50% higher than the starting

salary for UK computing graduates at the time. This indicates that graduates from the programme are highly valued by their employers. Good honours attainment has remained high for successive cohorts. It is noted that employers can use work-based learning to focus on cybersecurity applications to address their needs which provides direct benefits in increasing resilience. The coverage of cybersecurity across the curriculum does mean cybersecurity is not necessarily taught by cybersecurity specialists, but it is taught in subject context. One spin off benefit in relation to cybersecurity teaching is that the mainframe software engineering pathway has been able to incorporate highly specialised aspects of mainframe security which is delivered by industry experts.

Apprenticeships have been successful in attracting female students (approx. 35%) and students from Black, Asian and minority ethnic groups (approx. 25%), bringing much needed diversity into CS programmes. The courses therefore address one of the core skills objectives of the National Cyber Security Strategy which seeks to increase participation from under-represented groups.

3.3.4 Similar Practice in Other HEIs

Forty-five institutions deliver the DTS degree apprenticeship with representatives from across the university mission groups, further education colleges, and private providers. The level of take up suggests that the DTS course is valued by employers and higher education providers. Employers benefit from direct recruitment to their over-stretched development teams, the ability to shape computer science study to their needs. Higher education providers often experience benefits such as high-quality outcomes in terms of teaching metrics (e.g. high completion rates and employability), as well as strengthening industry links. The benefits of DAs, including the opportunity for the HEI to charge a full cost fee while no payment for study is made by students, make the DTS an attractive option. However, there are challenges in terms of the support needs for students who have to balance study alongside often a demanding work role.

3.3.5 Future Actions

It is critical that CS degrees incorporate current cybersecurity practice as both our reliance on software increases and the threat landscape becomes even more challenging. Currently, the core technical knowledge requirement relating to cybersecurity for students on DTS courses is to know and understand common vulnerabilities in computer networks including insecure coding and unprotected networks. The DTS apprenticeship standard is reviewed every 2 years, and this gives an opportunity for MMU to update the curriculum to reflect latest industry and academic trends in cybersecurity. We will continue to deliver a cross-curriculum approach for teaching cybersecurity that is built into the apprenticeship standard and supports cybersecurity learning in students' work contexts.

We will continue to expand DTS provision as it delivers both greater inclusivity and high graduate outcomes. MMU is continuing to develop its DA offer. The recent approval of DAs in Digital User Experience (UX) and Creative Digital Design extends the coverage to a broader range of digital careers.

3.3.6 Final Notes

DAs have been developed in partnership with employers which has ensured cybersecurity is covered and meets industry needs. DAs provide a means of working with employers to improve Equity, Diversity and Inclusion (EDI) outcomes for CS and is particularly important in meeting national diversity objectives for cybersecurity.

3.4 University of Bath

3.4.1 The Approach

The University of Bath is a high-tariff research-intensive university which, unusually among its peers, has a strong tradition of supporting industrial placements: positively helping students find placements (pre-Covid, and 99% of those who wanted placements had them) rather than relying on their social capital.

Bath does not aim to produce Cybersecurity specialists as such, though some graduates go into it, and even make headlines within a year of graduation [29].

3.4.2 Applied Modules/Programmes

The University has taught Cybersecurity since 2001, in two distinct forms.

Undergraduate The methodology to date has been to embed cybersecurity within the various compulsory courses taught. Some examples of this are:

1. Basic public-key cryptographic algorithms are taught within the second-year compulsory “Data Structures and Algorithms” unit;
2. Defensive programming is emphasised within the compulsory programming units;
3. SQL injection attacks are taught within the compulsory “Discrete mathematics and databases” unit.

The delivery of these materials varies: (1) security experts designed the material when he taught the unit, but the current lecturer delivers; (2) the lecturers deliver; (3) security experts deliver a “pop-up” lecture on the material. In addition, there is an optional final-year Cryptography unit.

Postgraduate In postgraduate education, Bath’s generalist MSc provision has had an (optional, taken by roughly half the students) module in Cybersecurity since 2001. This has carried over into both our Level 7 (MSc) DAs and online MSc provision, though staffing this has proved a challenge, especially for the security lecturers workload. In 2019, a colleague was brought back in to teach the module in preparation for this further rollout and to respond to complaints that the course had been too theoretical. As currently constituted, the generalist MSc has four assessments.

- (1) [30%] A group of roughly five research an issue, generally from OWASP Top 10 [41] or other OWASP resources, give a 20-minute (since Covid-19, recorded) presentation on the issue, aimed at an appropriate senior audience (e.g. Risk Committee or IT management), and answer questions. Each student is assigned three other presentations to watch, write a critical report, and prepare a question on.
- (2) [30%] Perform a (possibly mock) online purchase, while collecting both the HAR (HTML Archive) trace and a network-level trace (e.g. Wireshark). They then answer various questions on security of the purchase: who sees the PAN (credit card number), how is it protected in transit, what are the vulnerabilities to DNS hacking etc.
- (3) [20%] Group evaluation of these purchases. The group is asked to assume that the various sites the group members have used are being put forward as examples of their work by vendors, and to do a comparative evaluation from a security point of view.
- (4) [20%] Open-book online Examination. In this respect, Covid-19 has been an advantage, as such examinations are now ‘normal’, whereas previously they had to be disguised as a ‘class practical’, and had no support from the examinations office/process.

3.4.3 Future Actions

With the increasing emphasis on cybersecurity, we have taken advantage of a general curriculum restructure at Bath and will be moving to a compulsory cybersecurity module in year 2, with a syllabus similar to that of the postgraduate course aforementioned. This will leave items 2 and 3 as introduced above for Undergraduate programmes to continue: at the time of writing the future of item 1 is being discussed.

3.4.4 Final Notes

As a specific example of where general computing intersects with Cybersecurity concerns, we consider the example of databases/SQL injection. Despite being documented in 1998 [28] and widely lampooned in an XKCD cartoon [59], SQL

injection remains one of the favourite forms of cyber attack. This was partly down to the (failures of) the education system, as analysed by Taylor and Sakharkar [48, 49] in the context of United States education. More precisely they looked at the most recent editions of database textbooks used in the top 50 Computer Science departments in the United States (seven books used in 44 universities). They find “Five of the seven textbooks we looked at do not mention SQL injection at all. Five of these seven textbooks had chapters on both using other programming languages to access SQL databases, and on database security, making SQL injection highly relevant to their content”. Whilst most universities have some database coverage in their courses (and students will often have some database use in their projects), this tends to be very “cookbook” usage, and few universities have active database research groups. Hence both instructors and students tend to be more reliant on textbooks than in other areas. At Bath, the solution to this problem is that the database instructor, who admittedly is not an expert, gets one of the authors to give one lecture on SQL injection in the database course.

3.5 University of Glasgow

The research-led University of Glasgow attracts over 30,000 students from across the world. The School of Computing Science, situated within the College of Science and Engineering, is one of the oldest in the United Kingdom with approximately 70 academic members of staff spread across several research sections, staff that also support the design and delivery of many academic programmes, including undergraduate, postgraduate and research degrees.

The School of Computing Science currently offers a range of taught specific security courses, on topics including secure software engineering, forensics and usable security. The security-related topics are also covered and considered within non-security specific courses, such as networking, operating systems and professional issues. The mixture of specific and non-specific security courses affords students the opportunity to specialise in cyber security either as part of their undergraduate or postgraduate degree.

For the present case study, the focus is around a research seminar style course in cybersecurity that enculturates and engages senior undergraduate and postgraduate students in cybersecurity research. The rationale for the focus is to (1) present an example of cybersecurity education at senior students and (2) demonstrate an approach that harnesses the research-intensive environment to support students in advancing their knowledge and skills.

3.5.1 The Approach

The semester seminar course covers seven topics, such as differential privacy and federated learning as well as modelling trust in artificial intelligence, with a

dedicated academic lead for each topic. The course has no exam and is centred around coursework with three distinct assessments: individual research summaries, an individual research proposal and team delivery of a seminar.

For each topic, the academic lead sets four research papers in advance of a 2-hour seminar where the class discusses the paper and associated themes. The selected papers are typically considered seminal for the topic. The first assessment requires students to produce a summary of no more than 750 words prior to the seminar. The individual research summaries should offer a précis of each paper as well as any observed themes or interconnections between them. Students are provided support sessions on academic writing and reading research papers.

The second assessment requires students to self-organise into groups and to identify a seminar they want to deliver. The specific topic and week is confirmed with the team and they are expected to lead the seminar for the given week. The team are expected to produce a 20-minute opening presentation offering a summary and overview of the set research papers, 10-minute closing presentation on the intended lessons learned from the seminar as well as a seminar plan. The seminar plan should outline the activities that are designed to probe and deepen understanding of the papers and themes. The team is to deliver the seminar, but the academic lead can intervene to steer the session if it takes an inappropriate direction. For the purposes of assessment, a second academic joins the session to assess delivery of the seminar.

The third assessment is the individual research proposal of no more than 3000 words. Students are expected to devise a research proposal for original research investigation, not unlike the proposal that would be submitted alongside an application for a terminal research degree. Support and guidance is provided on writing research proposal, but peer-review is used to improve assessment literacy for the exercise [33]. Students are required to submit a draft proposal, review drafts from three peers as well as devise a plan for action to improve their draft upon receiving feedback. The expectation is that through observing the attempts of peers, reflecting on their own attempt and devising a plan of action—students will be able to refine expectations and improve their proposal [32].

3.5.2 Applied Modules/Programmes

The research seminar style course is weighted at 10-credits at Level 11 under the Scottish Credit and Qualification Framework (SCQF) and is targeted at senior undergraduate and postgraduate students. The course prepares students for considering a route into terminal research degree in cybersecurity or for roles in organisation that adopt a research culture for delivering on objectives.

3.5.3 Effects and Effectiveness

The research seminar style course is a relatively recent addition to the course portfolio. Consequently, sustained evidence of the course delivering on learning

objectives has yet to be established. Having said that, interim and informal feedback from staff and students suggest the course is successful in engaging students in research culture and activities. Moreover, the course provides a relatively unique experience in contrast to many taught options given its structure, style and focus on engaging with cybersecurity research and academics.

3.5.4 Similar Practice in Other HEIs

Research seminar style courses are not particularly novel, historically speaking. However, the popularity of such courses as part of undergraduate and postgraduate courses have dwindled as student enrolments have increased given the nature and expense in delivering high-quality variants of them. The present example is only partially viable as it is focused on a specific topic area, that is cybersecurity, rather than general computing science research.

Thimmaraju et al. [51] outline a recent example of a research seminar style course in cybersecurity to support students in developing critical skills as well as advancing knowledge. They report restricting enrolment to 15 students and students are expected to first identify a paper session at a leading cybersecurity conference, such as the ACM Conference on Computer and Communications Security (CCS). After identification of the paper session. Students are organised into teams of no more than three members. Teams are then allocated a paper to present on an aspect of research, such as methodology, presentation of results or how to read a research paper. Teams then present the topic to the rest of the class, effectively teaching each other and also receive feedback in terms of how they have considered the paper and presented it. Students then have the rest of the semester to read the three papers previously identified. Students have to prepare a 45-minute presentation in a conference style approach and provide three reviews. Thimmaraju et al. report the course attracts those students with a general interest in cybersecurity and they found the approach and structure novel and engaging. Although some students report they would like to be taught more material around the advanced topics emerging from research.

3.5.5 Future Actions

The next aspect is to assess the benefit of the course, but also consider how to motivate and support students that have a devised research proposal and how to support them into making an application for a terminal research degree.

3.5.6 Final Notes

It is important that students are not only afford opportunity to learn skills and knowledge, but also experiences and the opportunities to enculturate in environments that can support lifelong learning.

University of Glasgow offers an opportunity for students to experience rich research cultures and experiences. Opportunities that afford students to learn skills that are valuable in engaging in cybersecurity research but also in being ready for businesses and companies that adopted a research culture to deliver on business objectives.

3.6 University of Strathclyde

The University of Strathclyde is a former technical college which was founded in 1796, then gaining university status in 1962. The University is marketed as ‘the place of useful learning’ which reflects the intention to have an institution which supports a practical approach.

3.6.1 The Approach

Cybersecurity is taught across multiple Faculties, including Science and Engineering. The majority of cybersecurity provision is by the Department of Computer and Information Sciences. Within the Department of Computer and Information sciences, at the time of writing, there are six generalist programmes which cover cybersecurity, including BSc Computer Science, BSc Software Engineering, Digital & Technology Solutions (DA), BEng Computer and Electronic Systems, IT: Software Development (Graduate Apprenticeship), and a Masters in Software Development.

3.6.2 Applied Module/Programmes

The approach taken for the programmes is a generalist approach where security is taught predominantly within a single module in the programme. These are delivered by a single member of staff.

In the undergraduate degrees this module takes place in the final year, which is the fourth year for all but the DA programme which is in the third year. In contrast, the Masters in Software Development is a conversion Masters programme and is taught in the first semester. This programme accepts students with a strong undergraduate degree in a subject which is not computing science focused. This has implications for the depth and range of topics covered within the module due to the lack of pre-requisite knowledge. However, it still uses a single module approach. This requires a smaller number of staff with a security background.

To ensure module content is appropriate and does not fall out of line with industrial expectations, guest speakers from industry are invited each year to talk with students. This has the added benefit of consulting with those contacts to ensure module content and focus is appropriate. For example, recent discussions have

included the need to ensure appropriate consideration of concepts such that learners are able to adapt to new attacks and defence when they complete their studies. Another aspect is the need to automate analysis of security related data, which has been integrated into modules with students who have a coding background. This approach ensures content remains relevant for learners moving into the world of work.

The assessment for these modules differs depending on the cohort. The general structure is one piece of coursework worth 30%, and one unseen exam worth 70%. The exam has been a take home assessment for the past 2 years and this has worked well, since reduced need to memorise certain aspects allows learners to focus on the skills. Those with a programming background are provided with the option of a more technical focused coursework such as implementing a steganography algorithm, whilst those programmes with a less technical background are given coursework which is more research-based. In both approaches, the key aspect is reflecting on the work and how it fits in a given context. The intention is to ensure learners are fully engaged in critical thinking as it applies to security as developing a security mindset is a key objective of the modules.

The unseen exam could potentially be criticised for being inauthentic. However, the format is a scenario-based approach where students are provided with a real-world scenario and asked to make judgements and evaluate security questions as they relate to the scenario. This allows students to take their understanding and apply it to a new situation, hence increasing authenticity.

3.6.3 Effects and Effectiveness

In this approach, whilst some students may have a desire to go on to become specialists in the field, most simply require a background in key topics. As a result, the module takes a systems security approach covering key elements such as cryptography, network security and user authentication and access control.

However, a single module approach does also have benefits. For example, having a self-contained module means that students on a degree with this element as optional are able to avoid it should they wish to do so. Another benefit is the containment of specialist knowledge. If a distributed approach was used, members of staff with no security specialism would have to become familiar with security elements in order to teach. Alternatively, security staff could cover those elements. In either case, there is an associated overhead of managing such an approach which also has implications for accreditation. If the content is self-contained, then ensuring appropriate requirements are met is easier than looking at many modules.

3.6.4 Similar Practice in Other HEIs

A single module approach within generalist programmes is not uncommon within the UK [10]. Using a single module to primarily deliver core cybersecurity has a

number of challenges. Firstly, students often come to the class with their own pre-conceived notions of cyber security. This is of particular note when it is part of an undergraduate degree. This means the lecturer has to justify selection or exclusion of topics or skills which can cause some dissatisfaction for students when their expectations are not met. It can also mean students are waiting a considerable time to cover these elements, building expectations yet higher or meaning students aim to explore the topic on their own which can cause conflict with the delivery of the module. Students on a Masters conversion programme often struggle to adjust to the content in such a short timeframe (10 weeks), which is amplified by incorporating all elements into a single module. If instead it were distributed across modules, it could be covered incrementally over the course of the programme, likely making it more accessible to the diverse student body.

3.6.5 Future Actions

As the department expands its portfolio, the requirement for cybersecurity modules is increasing. As a result, resources are developed in a modular fashion such that elements from a larger set of resources can be identified for specific programmes. This already happens to some extent in the Undergraduate and conversion programmes, where there are two possible routes. One for students with little or no technical background, and the other for those with known pre-requisite knowledge. This approach works well in that it can be adapted more easily, and has less of a workload than multiple staff delivering similar modules, but it does have an overhead for management and introduces challenges in designing content suitable for diverse student bodies.

Moving forward it will be necessary to review cyber provision within undergraduate programmes due to the increased emphasis on cybersecurity in the BCS accreditation guidance. The change in guidance in 2020 means that the quantity of cybersecurity is unlikely to be manageable within a single module. Adjustments to existing modules to incorporate elements such as risk management is likely but will require appropriate oversight to implement. This would then permit cross-curricular cybersecurity whilst maintaining a more focused module which covers key elements which do not necessarily fit within other modules. This approach is similar to that proposed at Northumbria University as discussed in Sect. 3.1.

3.7 University of Gloucestershire

3.7.1 The Approach

Cyber Scheme [50] was established to increase choice in the provision of NCSC (formerly Communications-Electronics Security Group (CESG)) certification of practitioner and senior penetration testers to the standard required to undertake

formal government and public sector work. It started with a not for profit ethos and an aim to increase accessibility to people from all backgrounds and capabilities to the world of technology assurance. It was established by two Small and Medium-sized Enterprises (SME) security testing companies who had a passion for making assessments more accessible and relevant as the cybersecurity skills gap grew wider. The University of Gloucestershire teamed up with the Cyber Scheme to embed the training and assessment as part of the degree cybersecurity offer. Students are given the opportunity to be trained and achieve a Cyber Scheme certification on top of their degree, which makes them highly employable within the security sector.

3.7.2 Applied Modules/Programmes

Cyber (compared with many) is a relatively immature industry and whilst there have been many advances in best practice, guidance and standards, the Professional Certifications space has evolved in what is broadly an unregulated labour skills market. The NCSC has a statutory responsibility to ensure that Government and public sector organisations are adequately protected against people, process and technology risks. To support this they create the Cyber Scheme of assured suppliers and professionals.

Like many employers, they need confidence in the competence of the people and the businesses representing that role within the commercial sector. Whilst there is some space for recognition of qualifications the structure of assessments are very specific for NCSC and as such they have selected a limited number of Assured suppliers of assessments. An analogue of this might be something like the Driver and Vehicle Licensing Agency (DVLA) driving examiners process. To get a licence you need to pass the approved assessment.

The pace of technology change does create challenges even in that space with more autonomous safety systems so what the driving test requires in terms of competence measure will be very different in 3 years than it is today. The same applies to the future of technology assurance and the Penetration testing discipline. What we have learned about technology innovation is that we have to live with different risks. Patching is part of daily life, because no one can eliminate cyber risk.

3.7.3 Effects and Effectiveness

It works in the sense that it is not trying to solve the worlds problems in skills and competencies space in one go. The number of Cyber Scheme Certified individuals is in 100s not 1000s. It also works because all certified individuals undertaking work are subjected to quality assurance of the work they do.

The Cyber Scheme's assessment seeks to replicate as close to a real world engagement that a tester might be exposed to. It is not dissimilar to an Job Interview Assessment Centre model. Most employers use a range of different candidate

selection processes but the core elements are still explored (Knowledge, Skills and Behaviours). In our case the output is people certified to a standard that the NCSC trusts. Assessments are not solely paper based, but they include interviews and their workflow is monitored continuously by Assessors drawn from the assured scheme with a minimum of 5 years experience as a Cyber Scheme Team Leader to assess at the senior level and 2 years at the practitioner level.

3.7.4 Similar Practice in Other HEIs

Different nations have different approaches to certification but in the UK NCSC had appointed three assessment bodies The Council for Registered Ethical Security Testers (CREST), Cyber Scheme and Tiger Scheme (University of Glamorgan). Tiger has recently ceased operating examinations.

3.7.5 Future Actions

Given the adaptive nature of cyber threat, the normalisation of integrated digital ecosystems driving every element of life, and unconstrained innovation, the nature of risk is driving the need to improve skills and competence to greater levels. Assessments covering adversarial behaviours, Internet of Things (IoT), Industrial IoT (IIoT), Industrial Control System (ICS), autonomous mobility, service virtualisation and data integrity services are all areas where we need confidence in the assurance decisions reached. Therefore the future of technology assurance is core to our plans.

Every citizen is a potential victim of cyber crime now, every business a hostage to opportunistic crime and targeted crime, and at the same time innovation in technology continues to be based on there being a level of personal responsibility to manage technology risk. The pace of change technically is moving faster than the ability of people to understand and adapt to managing risk and resilience in the digital world. The Cyber Scheme is, therefore, partnering with the Cyber Trust (a charity focused on dealing with social harms for young persons through digital connectivity) and the Cyber Security Challenge which has many years of experience in delivering education and development programmes for new talent pipelines and also youth intervention projects with the National Crime Agency (NCA) on trying to focus talent on good outcomes vs. criminal outcomes.

The strong relationship with the University of Gloucestershire, and the University of Warwick, was built up over time to ensure we understand fully how educational standards are evolving and also working in partnership to narrow the gap between academic assessment and industry measures of competence. There are modern apprentice programmes which have great potential and Cyber Scheme is keen to support that learning with industry sessions and will work with our close partners on that in the coming year. It is important to look at how we develop competence at

all levels in all walks of life so we will develop projects and programmes of activities and certifications to underpin that and support employers and employees at all levels in society.

3.7.6 Final Notes

Grand plans usually need grand funding sources and support. We are working with industry partners to seek support through gifting time and money to help the projects develop. It would be good to promote best practice and also seek sponsorship from other organisations to achieve specific aims. We also recognise the need for partnership approaches and the Cyber Scheme are a member of the Cyber Security Council to help in the discussion and debate about the future of the profession but more importantly to ensure that some sectors of society do not get excluded from being considered to be professional at what they do.

Competence exists at many levels each as valuable as the other. An industry that feels elitist will never deliver the societal outcomes that are necessary. The cyber health of the nation is critical but the challenge we face today is that much of the outreach for health support is private sector. NCSC is growing its interventions but clearly they are not the National Health Service (NHS). The UK employs circa 1.5 million professionals in the NHS service portfolio to look after the physical and mental health of the UK. We need as many to look after the cyber health of the UK in our opinion but in a way that they all see themselves as part of a structure/community not just living in silos.

4 Key Themes from Case Studies

Treatment of cybersecurity teaching and learning has been described in the case studies from seven universities above. The case studies were chosen to reflect a cross-section of UK universities. They include a mix of modern universities which focus on applied research with a strong emphasis on teaching and long-established research-intensive universities. Key findings from the case studies are summarised in Table 2, with the main themes emerging from these case studies listed. In this table, ‘Cross-curricular’ represents that cybersecurity topics are covered in more than one module and delivered in context of module e.g. vulnerabilities in web Apps created by injecting code taught in a Web Development module; ‘Dedicated module’ indicates cybersecurity is covered in one dedicated module; and UG and PG stand for Undergraduate and Postgraduate (i.e. MSc), respectively.

Table 2 Key themes identified from the case studies

University	UG /PG	Delivery	Accreditation	Outcomes
Northumbria	UG	Cross-curricula	BCS	<p><i>Positive:</i> Design and deliver in collaboration with industry. Security learned in a discipline context so ubiquitous</p> <p><i>Negative:</i> Assessment distributed across programme so can be seen as less significant than other curricula areas. Within each module a small curricula area that some strategic students perceive as optional, which may be exacerbated when delivered by industrialists as can be seen as an extension activity. Requires management to assure continued coverage</p>
Sunderland	UG	Cross-curricula and Dedicated module	BCS	<p><i>Positive:</i> Improved employability opportunities for CS students—both in terms of ‘traditional’ CS jobs, but also opening access to cyber jobs. Many students used cybersecurity to enhance their final year projects</p> <p><i>Negative:</i> Some programmes (Games Computing) not so clear upon its relevance</p>
MMU	UG	Cross-curricula	BCS	<p><i>Positive:</i> Industry designed degree apprenticeship, a high proportion of female students, cyber learnt in a work context</p> <p><i>Negative:</i> Not necessarily taught by cybersecurity experts</p>
Bath	UG	Cross-curricula	BCS	Moving to compulsory second-year module (as well). Uses “pop-up” lecturers where appropriate
	PG	Optional module		Payment card exercise very successful. Several students access cybersecurity careers upon graduation
Strathclyde	UG	Dedicated module	BCS	<p><i>Positive:</i> Consistent delivery across programmes with regular industrial input</p> <p><i>Negative:</i> Demanding course for both staff and students that does not scale particularly well</p>
Glasgow	UG	Dedicated module	BCS	<p><i>Positive:</i> Rich experience that affords students to harness a rich research environment to advance knowledge and skills</p> <p><i>Negative:</i> Demanding course for both staff and students that does not scale particularly well</p>

(continued)

Table 2 (continued)

University	UG /PG	Delivery	Accreditation	Outcomes
Gloucestershire	PG	Cross-curricula	NCSC	<i>Positive:</i> Rich curriculum mapped against CybBok, and the certification is regarded as a strong indicator of quality by students and employers alike
	UG	Cross-curricula	Cyber Scheme	<i>Positive:</i> The Cyber Scheme certification makes graduates highly employable to security firms <i>Negative:</i> Not all students manage to pass the certification test. There is a tension between covering the requirements of the certification and space available to cover other aspects of the degree programme

4.1 Cyber Security Content Delivery

Three main approaches were taken to delivering cybersecurity content, in one approach teaching was distributed across the curriculum and in the other approach cybersecurity was taught in a single dedicated module and the third way was a hybrid of the two with principles embedded across the curriculum and then brought together in a specialist module, normally in final year.

Analysis of the case studies suggests that the main benefit of the cross-curriculum approach is that cybersecurity is taught in context allowing threats/vulnerabilities to be considered alongside related content, for example consider cybersecurity in data base design or defensive programming in programming modules. This is consistent with a move to cybersecurity becoming ‘mainstreamed’ in CS curricula and practice. However, this approach relies on CS faculty building up cybersecurity expertise and developing cyber knowledge applied to their area of the discipline. This potentially places increased demands on academic staff working in fast-changing subject areas. It may also mean that students have difficulty in integrating cybersecurity knowledge and recognising its overall significance because they see it as a subset of the subject they are looking at.

The use of a dedicated module has the merit of enabling a consistent approach to teaching cybersecurity delivered by a specialist, ensuring students are aware of the critical nature of the topic. The negative aspects of using a dedicated module noted were: a high reliance on one member of staff, single point of failure, places a high demand on staff and students which does not scale well. The case studies indicate that both approaches can produce good student outcomes, but each require mitigations to ensure success. In particular, each delivery strategy requires different approaches to managing staff resources to ensure the right expertise is available. It is interesting to note that four institutions (Bath, Northumbria, Sunderland and

Strathclyde) adopted (or are moving towards) a hybrid approach incorporating a dedicated cybersecurity module alongside cross-curricular treatment, reflecting the increased importance of security to CS graduates.

4.2 Employer Involvement in Curriculum Design

A common theme in the case studies was the involvement of industry in the co-design of the curriculum, and in some cases actual development and delivery of material. This was achieved through employer groups either linked to the university e.g. Industrial Advisory Board as at Sunderland or a national group as in the case of MMU's DAs. MMU and Sunderland cite employer engagement in design of curriculum as a mechanism for improving graduate outcomes. Employer delivery of cybersecurity lectures was used by two institutions (Northumbria and Strathclyde) as a way covering specialist topics and enriching the curriculum. Employer engagement was noted as key feature driving the success of programmes.

4.3 Employability

The case studies frequently mention the benefits of their treatment of cybersecurity for students' employment prospects. It is difficult to determine causality to any one initiative when considering employability. One case study, Sunderland, did track improvements in employability to more significant treatment of cybersecurity. Other case studies note a move to more significant coverage of cybersecurity in CS programmes is required to create graduates that meet the needs of industry.

4.4 Accreditation

UK universities mainly use the QAA benchmark, which is itself cross references the ACM/IEEE curricula recommendations [1, p35], to develop curriculum. The enhancements in these standards over the last 10 years, outlined in Sects. 2.3 for the QAA and 2.4 for ACM, enforces increased coverage of cybersecurity in CS curricula. Gaining accreditation is optional for CS programmes but is sought by universities to add a kite mark of quality to increase attractiveness to employers and students. All the programmes in the seven case studies had achieved professional accreditation. Six have BCS accreditation, which as noted in Sect. 2.2, strengthened its cybersecurity requirements in 2015. Whilst BCS accreditation is gained for wider reasons, increased emphasis on cybersecurity is consistent with industry needs. One university, Strathclyde, noted explicitly that BCS accreditation was a driver for reviewing cybersecurity coverage indicating the benefit for ensuring necessary

curriculum content. One university, Gloucestershire, had gained Cyber Schemes cybersecurity Certification for its undergraduate provision and built their CyBOK certification into its postgraduate curriculum. These specialist accreditations are cited as increasing employability, particularly in cybersecurity roles. However more cybersecurity curriculum content for the NCSC certifications created a tension in covering other legitimate CS topics.

In summary, there was no single dominant approach to delivering cybersecurity within CS programmes among the case studies. A variety of teaching methods were employed including delivery by visiting professors and industry experts, work-based learning and a seminar-based approach to enculturate cybersecurity research among students. It is clear from the case studies that universities are working with employers and professional bodies to increase the level of cybersecurity coverage in CS programmes to enhance student employability and meet the needs of industry.

5 Conclusions and Recommendations

There appears to be a growing global consensus that (cyber) security is a discipline area that should permeate computing and hence be included within all computing degree qualifications. Most notably for a UK context, this is the view argued by the curricula recommendations from ACM/IEEE (which are cross-referenced by the QAA Benchmark Statement), the BCS, and the UK Government as promoted by NCSC accreditation. As highlighted at the start of this chapter, this is in the wider context of major national and international curriculum and qualifications reform initiatives in computer science education, from early-years through to university-level. We are also cognisant of the emerging longer-term impact of the COVID-19 pandemic on education across all levels and settings, but especially computer science as a discipline.

From the case studies presented in the chapter the emergent good practice approach for how to deliver cybersecurity content for mainstream undergraduate computing programmes appears to be to include a module focusing directly upon cybersecurity and to augment this with cross-curricula coverage in other modules where security is pertinent. For mainstream postgraduate computing qualifications the emergent practice appears to be less consistency and divergent practices are being employed.

Accreditation by professional, statutory and regulatory bodies is not without criticism, such as unnecessary bureaucratic and constrain innovation amongst other. However, the value of professional body degree accreditation regimes as a kite-marking exercise and to support a globally-portable and recognised workforce remains high. This chapter has also discussed the value and practice of professional accreditation regarding cybersecurity contents. NCSC accreditation is aimed at specialist degree provision in the sense of either security focused degrees or mainstream computing degrees with a significant security focus. The accreditation

expectations provide effective and actionable guidance for the curricula design of programmes with this cybersecurity focus.

BCS accreditation is more general aimed at the full spectrum of possible computing degrees including those with a security focus but by no means limited to those. From a security perspective the intention is to assure a minimum threshold of security coverage is present, with that threshold being that which a mainstream computing/IT professional should be aware of to enable them to function in the modern environment. Such knowledge is intended to assist in the prevention of security flaws but also to provide enough knowledge to know when specialist input needs to be sought.

The addition of cybersecurity to mainstream computing curricula adds to the ongoing challenge of what to not include within a particular programme. Other related questions being should all programmes embed programming or machine learning or data science or human-computer interaction, etc. The discipline is very broad, and no single programme can hope to cover all areas. The ACM 2020 Curricula provides helpful guidance as to what might be the discipline limits for computing programmes. Whilst hybrids between the areas are possible and curricula innovations are to be encouraged there is a useful debate as to what the core components of all computing qualifications should be for the time being, but this will be an ever evolving concept along with the ever shifting landscape of computing technologies.

Acknowledgments This work has been partially supported by the Royal Academy of Engineering through the Visiting Professors Scheme (Bringing Industry into Academia: VP1920\6\90) and the Industry Academia Partnership Programme (IAPP1\100077).

References

1. ACM/IEEE-CS Task Force: Computing Curricula 2020 (CC2020): Paradigms for Global Computing Education. Tech. rep., ACM and IEEE-CS (2020). <https://www.acm.org/binaries/content/assets/education/curricula-recommendations/cc2020.pdf>
2. Adeniji, D.: FireEye:- Sunburst Attack. <https://learningintheopen.org/2020/12/17/fireeye-sunburst-attack/> (2020)
3. BCS, The Chartered Institute for IT: Guidelines on course accreditation (January 2020). <https://www.bcs.org/media/1209/accreditation-guidelines.pdf> (2022)
4. Brown, N.C.C., Kölling, M., Crick, T., Peyton Jones, S., Humphreys, S., Sentance, S.: Bringing Computer Science Back Into Schools: Lessons from the UK. In: Proceedings of 44th ACM Technical Symposium on Computer Science Education (SIGCSE'13), pp. 269–274. ACM (2013). <https://doi.org/10.1145/2445196.2445277>
5. Brown, N.C.C., Sentance, S., Crick, T., Humphreys, S.: Restart: The Resurgence of Computer Science in UK Schools. *ACM Transactions on Computer Science Education* **14**(2), 1–22 (2014). <https://doi.org/10.1145/2602484>
6. Crick, T.: COVID-19 and Digital Education: A Catalyst for Change? *ITNOW* **63**(1), 16–17 (2021). <https://doi.org/10.1093/itnow/bwab005>
7. Crick, T., Davenport, J.H., Hanna, P., Hayes, A., Irons, A., Miller, K., Prickett, T., Ward, R., Allen, B., Patil, B., Payne, S.: Co-Constructing a Community of Practice for Early-Career Computer Science Academics in the UK. In: Proceedings of Computing Education Practice (CEP'22). ACM (2022). <https://doi.org/10.1145/3498343.3498349>

8. Crick, T., Davenport, J.H., Hanna, P., Irons, A., Pearce, S., Prickett, T.: Repositioning BCS Degree Accreditation. *ITNOW* **62**(1), 50–51 (2020). <https://doi.org/10.1093/itnow/bwaa023>
9. Crick, T., Davenport, J.H., Hanna, P., Irons, A., Prickett, T.: Computer Science Degree Accreditation in the UK: A Post-Shadbolt Review Update. In: *Proceedings of Computing Education Practice (CEP'20)*, pp. 1–4. ACM (2020). <https://doi.org/10.1145/3372356.3372362>
10. Crick, T., Davenport, J.H., Hanna, P., Irons, A., Prickett, T.: Overcoming the challenges of teaching cybersecurity in uk computer science degree programmes. In: *Proceedings of 50th Annual Frontiers in Education Conference (FIE'20)*, pp. 1–9 (2020). <https://doi.org/10.1109/FIE44824.2020.9274033>
11. Crick, T., Davenport, J.H., Hayes, A., Irons, A., Prickett, T.: Supporting Early-Career Academics in the UK Computer Science Community. In: *Proceedings of Computing Education Practice (CEP'21)*. ACM (2021). <https://doi.org/10.1145/3437914.3437977>
12. Crick, T., Davenport, J.H., Irons, A., Pearce, S., Prickett, T.: Maintaining the Focus on Cybersecurity in UK Higher Education. *ITNOW* **61**(4), 46–47 (2019). <https://doi.org/10.1093/itnow/bwz110>
13. Crick, T., Davenport, J.H., Irons, A., Prickett, T.: A UK Case Study on Cybersecurity Education and Accreditation. In: *Proceedings of 49th Annual Frontiers in Education Conference (FIE'19)*, pp. 1–9. IEEE (2019). <https://doi.org/10.1109/FIE43999.2019.9028407>
14. Crick, T., Knight, C., Watermeyer, R.: Reflections on a Global Pandemic: Capturing the Impact of COVID-19 on the UK Computer Science Education Community. In: *Proceedings of UK and Ireland Computing Education Research Conference (UKICER'22)*. ACM (2022). <https://doi.org/10.1145/3555009.3555027>
15. Crick, T., Knight, C., Watermeyer, R., Goodall, J.: The Impact of COVID-19 and “Emergency Remote Teaching” on the UK Computer Science Education Community. In: *Proceedings of UK and Ireland Computing Education Research Conference (UKICER'20)*. ACM (2020). <https://doi.org/10.1145/3416465.3416472>
16. Crick, T., Prickett, T., Davenport, J.H., Irons, A.: Assessing the Value of Professional Body Accreditation of Computer Science Degree Programmes: A UK Case Study. In: *Proceedings of 25th Annual Conference on Innovation and Technology in Computer Science Education (ITiCSE'20)*. ACM (2020). <https://doi.org/10.1145/3341525.3393980>
17. Crick, T., Prickett, T., Bradnum, J.: Exploring Learner Resilience and Performance of First-Year Computer Science Undergraduate Students during the COVID-19 Pandemic. In: *Proceedings of 27th Annual Conference on Innovation and Technology in Computer Science Education (ITiCSE'22)*, pp. 519–525. ACM (2022). <https://doi.org/10.1145/3502718.3524764>
18. Davenport, J.H., Crick, T.: Cybersecurity Education and Formal Methods. In: *Formal Methods – Fun for Everybody, Communications in Computer and Information Science*, vol. 1301. Springer (2021). https://doi.org/10.1007/978-3-030-71374-4_8
19. Davenport, J.H., Crick, T., Hourizi, R.: The Institute of Coding: A University-Industry Collaboration to Address the UK’s Digital Skills Crisis. In: *Proceedings of IEEE Global Engineering Education Conference (EDUCON'20)*, pp. 1400–1408. IEEE (2020). <https://doi.org/10.1109/EDUCON45650.2020.9125272>
20. Davenport, J.H., Hayes, A., Hourizi, R., Crick, T.: Innovative Pedagogical Practices in the Craft of Computing. In: *Proceedings of 4th International Conference on Learning and Teaching in Computing and Engineering (LaTiCE'16)*, pp. 115–119 (2016). <https://doi.org/10.1109/LaTiCE.2016.38>
21. Department of Digital, Culture, Media and Sport : Independent report: CyberFirst Evaluation. <https://www.gov.uk/government/publications/independent-evaluations-of-cyber-discovery-and-cyberfirst-programmes/cyberfirst-evaluation> (2021). UK Government
22. Department of Digital, Culture, Media and Sport: Cyber Discovery Evaluation. <https://www.gov.uk/government/publications/independent-evaluations-of-cyber-discovery-and-cyberfirst-programmes/cyber-discovery-evaluation> (2021). UK Government
23. Department of Digital, Culture, Media and Sport: Cyber Security Breaches Survey 2021. <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021> (2021). UK Government

24. Engineering Council: Guidance on Security. <https://www.engc.org.uk/security> (2021)
25. Harvey, L.: The power of accreditation: views of academics. *Journal of Higher Education Policy and Management* **26**(2), 207–223 (2004). <https://doi.org/10.1080/1360080042000218267>
26. Irons, A., Crick, T.: In: *Higher Education in a Post-COVID World: New Approaches and Technologies for Teaching and Learning*, chap. Cybersecurity in the Digital Classroom: Implications for Emerging Policy, Pedagogy and Practice, pp. 231–244. Emerald (2022). <https://doi.org/10.1108/978-1-80382-193-120221011>
27. (ISC)², CPHC: Cybersecurity Principles and Learning Outcomes for Computer Science and IT-Related Degrees: A Resource for Course Designers and Accreditors. <https://cphcuk.files.wordpress.com/2015/06/j0028-isc2-white-paper-a4-v5-260515lr.pdf> (2015)
28. J. Forristal (signing as rain.forest.puppy): NT Web Technology Vulnerabilities. <http://phrack.org/issues/54/8.html> (1998)
29. Jones, P.: How Digital Forensics Expert Mustafa Lattouf is Changing the Game in Cybersecurity. <https://www.techtimes.com/articles/261921/20210624/how-digital-forensics-expert-mustafa-lattouf-is-changing-the-game-in-cybersecurity.htm> (2021)
30. Kneale, P.E.: The rise of the ‘strategic student’: How can we adapt to cope? In: *Facing up to radical changes in universities and colleges*, pp. 119–130. Routledge (2012)
31. Knight, J.: The international race for accreditation. *International Higher Education* **40**, 2–3 (2015). <https://doi.org/10.6017/ihe.2005.40.7490>
32. Li, L., Liu, X., Steckelberg, A.L.: Assessor or assessee: How student learning improves by giving and receiving peer feedback. *British Journal of Educational Technology* **41**(3), 525–536 (2010). <https://doi.org/10.1111/j.1467-8535.2009.00968.x>
33. Maguire, J., English, R.: Opportunities to fail: Using peer-review to support assessment literacy in cyber security. In: *Proceedings of 21st Koli Calling International Conference on Computing Education Research*. ACM (2021). <https://doi.org/10.1145/3488042.3489967>
34. Ministry of Housing, Communities & Local Government: English indices of deprivation 2019. <https://www.gov.uk/government/statistics/english-indices-of-deprivation-2019> (2019). UK Government
35. Moller, F., Crick, T.: A University-Based Model for Supporting Computer Science Curriculum Reform. *Journal of Computers in Education* **5**(4), 415–434 (2018). <https://doi.org/10.1007/s40692-018-0117-x>
36. Murphy, E., Crick, T., Davenport, J.H.: An Analysis of Introductory Programming Courses at UK Universities. *The Art, Science, and Engineering of Programming* **1**(2)(18) (2017). <https://doi.org/10.22152/programming-journal.org/2017/1/18>
37. Mutereko, S.: Analysing the accreditation of engineering education in south africa through foucault’s panopticon and governmentality lenses. *Assessment & Evaluation in Higher Education* **43**(2), 235–247 (2018). <https://doi.org/10.1080/02602938.2017.1330395>
38. National Cyber Security Centre: NCSC Annual Review 2021. <https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021> (2021)
39. National Cyber Security Centre: NCSC-certified degrees. <https://www.ncsc.gov.uk/information/ncsc-certified-degrees> (2022)
40. Oudshoorn, M.J., Thomas, S., Raj, R.K., Parrish, A.: Understanding the new abet computer science criteria. In: *Proceedings of the 49th ACM Technical Symposium on Computer Science Education (SIGCSE’18)*, pp. 429–434. ACM (2018). <https://doi.org/10.1145/3159450.3159534>
41. OWASP: OSWASP Top Ten. <https://owasp.org/www-project-top-ten/> (2021)
42. Parrish, A., Impagliazzo, J., Raj, R.K., Santos, H., Asghar, M.R., Jøsang, A., Pereira, T., Stavrou, E.: Global perspectives on cybersecurity education for 2030: A case for a meta-discipline. In: *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE’18)*, pp. 36–54. ACM (2018). <https://doi.org/10.1145/3293881.3295778>
43. Quality Assurance Agency: Computing: Subject Benchmark Statement. <https://www.qaa.ac.uk/quality-code/subject-benchmark-statements/computing> (2022)
44. Rashid, A., Martin, A., Schneider, S., Cherdantseva, Y., Chapman, R., Krotofil, D.M.: CyBOK. <https://www.cybok.org> (2022)

45. Sentance, S., Kirby, D., Quille, K., Cole, E., Crick, T., Looker, N.: Computing in School in the UK & Ireland: A Comparative Study. In: Proceedings of UK and Ireland Computing Education Research Conference (UKICER'22). ACM (2022). <https://doi.org/10.1145/3555009.3555015>
46. Siegel, A., Zarb, M., Alshaigy, B., Blanchard, J., Crick, T., Glassey, R., Holt, J.R., Latulipe, C., Riedesel, C., Senapathi, M., Simon, Williams, D.: Teaching through a Global Pandemic: Educational Landscapes Before, During and After COVID-19. In: Proceedings of the 2021 Working Group Reports on Innovation and Technology in Computer Science Education (ITiCSE-WGR'21) (2021). <https://doi.org/10.1145/3502870.3506565>
47. Simon, Mason, R., Crick, T., Davenport, J.H., Murphy, E.: Language Choice in Introductory Programming Courses at Australasian and UK Universities. In: Proceedings of 49th ACM Technical Symposium on Computer Science Education (SIGCSE'18), pp. 852–857. ACM (2018). <https://doi.org/10.1145/3159450.3159547>
48. Taylor, C., Sakharkar, S.: Best paper at SIGCSE 2019 in the curriculum initiatives track: 'drop table textbooks;--: An argument for SQL injection coverage in database textbooks. ACM Inroads **10**(2), 58–64 (2019). <https://doi.org/10.1145/3324897>
49. Taylor, C., Sakharkar, S.: 'drop table textbooks;--: An argument for sql injection coverage in database textbooks. In: Proceedings of the 50th ACM Technical Symposium on Computer Science Education (SIGCSE'19), pp. 191–197. ACM (2019). <https://doi.org/10.1145/3287324.3287429>
50. The Cyber Scheme: The Cyber Scheme. <https://thecyberscheme.org/> (2022)
51. Thimmaraju, K., Fietkau, J., Ganji, F.: Towards an Insightful Computer Security Seminar. <https://doi.org/10.48550/arXiv.2003.11340> (2020)
52. Tryfonas, T., Crick, T.: Smart Cities, Citizenship Skills and the Digital Agenda: The Grand Challenges of Preparing the Citizens of the Future. Tech. rep., UK Government Office for Science and Department for Business, Innovation & Skills (2015). <https://www.gov.uk/government/publications/future-of-cities-smart-cities-citizenship-skills-and-the-digital-agenda>
53. Tryfonas, T., Crick, T.: Public Policy and Skills for Smart Cities: The UK Outlook. In: Proceedings of 11th International Conference on PErvasive Technologies Related to Assistive Environments (PETRA'18), pp. 116–117. ACM (2018). <https://doi.org/10.1145/3197768.3203170>
54. UK Government: Cyber Security Strategy. <https://www.gov.uk/government/publications/cyber-security-strategy> (2011)
55. UK Government: Cyber Security Strategy. <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021> (2011)
56. Ward, R., Phillips, O., Bowers, D., Crick, T., Davenport, J.H., Hanna, P., Hayes, A., Irons, A., Prickett, T.: Towards a 21st Century Personalised Learning Skills Taxonomy. In: Proceedings of IEEE Global Engineering Education Conference (EDUCON'21), pp. 344–354. IEEE (2021). <https://doi.org/10.1109/EDUCON46332.2021.9453883>
57. Watermeyer, R., Crick, T., Knight, C., Goodall, J.: COVID-19 and digital disruption in UK universities: afflictions and affordances of emergency online migration. Higher Education **81**, 623–641 (2021). <https://doi.org/10.1007/s10734-020-00561-y>
58. Watermeyer, R., Shankar, K., Crick, T., Knight, C., McGaughey, F., Hardman, J., Suri, V., Chung, R., Phelan, D.: 'Pandemia': A reckoning of UK universities' corporate response to COVID-19 and its academic fallout. British Journal of Sociology of Education **42**(5–6), 651–666 (2021). <https://doi.org/10.1080/01425692.2021.1937058>
59. XKCD: Cartoon 327. <https://xkcd.com/327/> (2007)

Using the Delphi Method to Elicit Requirements for an International Master's Program in Information Security Management



Fredrik Karlsson, Karin Hedström, and Ella Kolkowska

1 Introduction

Universities must regularly assess the study programs they offer, to provide a relevant and competitive educational portfolio. Örebro University in Sweden is no exception. We continuously make assessments of the relevance and quality of our study programs. In 2015, the existing master's program in Information Systems had experienced a declining number of students for several years. Therefore, a decision was made to design and launch a new program with a different study profile. The Informatics department at Örebro University, which is hosting the master's program in Information Systems, executed a SWOT-analysis to identify a potential profile for the new master's program. This analysis showed that one of the department's research strengths is information security management. At the same time, there were few available national and international master's programs in Sweden and Europe with such a profile. Considering companies and public organizations' critical reliance on information technology and information, together with an increase in information security threats [1–3], we identified a need for information security specialists. The university therefore decided to develop a 2-year International Master's program in Information Systems with a specialization in information security management, to be launched in fall 2018.

University study programs needs to be based on research knowledge as well as have practical relevance. Requirements that increase the practical relevance are essential to make graduated students employable and for the organizations that are going to recruit students. Consequently, practical relevance plays a key role in state-of-the-art curriculum development considerations. Having said that,

F. Karlsson (✉) · K. Hedström · E. Kolkowska
Örebro University, Informatics, Örebro, Sweden
e-mail: fredrik.karlsson@oru.se; karin.hedstrom@oru.se; ella.kolkowska@oru.se

elicitation of requirements that enhance practical relevance is no easy task. We know, from existing research on information systems that there are no ready-made requirements ‘out there’ to be collected [4]. Instead, requirements are formulated and (re-)negotiated together with the stakeholders [5–7]. Consequently, there is a need to employ an effective requirements-elicitation process; preferably a process that can be efficiently repeated to keep track of changing requirements.

During the development of the International Master’s Program in Information Security Management we employed the Delphi method [8, 9]. The aim of this chapter is to describe the process of eliciting and prioritizing course requirements using an adapted Delphi method and to present lessons learned. Our hope is that our contribution can help other educational institutions elicit requirements and increase the practical relevance of their study programs. Although we used an adapted Delphi method in the development of our master’s program in information security management, the lessons learned are not bound to this particular context. Instead, we believe that they are applicable to requirements elicitation of any kind of study program for which the intention is to use the Delphi-method.

The chapter proceeds as follows. In the next section, we present the case context which is important for the interpretation of the development work, i.e., to make it possible to assess the transferability of the adapted method and the lessons learned. In the third section, we expand on the notion of the Delphi method and how it was implemented during the development of the master’s program. The fourth section contains an illustrative example of elicited requirements and how they were used in the development of the study program curriculum and a course syllabus. With this foundation, we provide lessons learned in the fifth section. Finally, we provide a short conclusion and discussion of the usefulness of our contribution.

2 Case Background

2.1 Research and Education Environment

Örebro University is a mid-sized Swedish university, which was founded in 1999. However, its roots as an educational institution date back to the 1960s. There are three faculties at Örebro University. The faculties oversee the academic and pedagogical activities within their respective fields, and each faculty encompasses several schools. In total, the university has eight schools. The Informatics department belongs to the School of Business, which is part of the Faculty of Business, Science and Engineering. The Business school’s mission is to carry out high quality research and in close interaction between staff, students and industry, develop professional employable individuals who make a difference in work and society; thus, practical relevance has a central position in all study programs offered.

At the time when the development work started, the Informatics department had 14 faculty members and 14 PhD students. The head of department is responsible for education and staffing. Education-wise, the Informatics department hosted two study programs; one bachelor’s program and one master’s program. Each

program is coordinated by a program manager, who manages the overall program administration, which includes coordination with the course coordinators. The existing master's program was launched in 2006 and recruited both national and international students. After several successful years, the number of applicants had started to decline, which triggered the redesign of the program.

The research in Informatics at Örebro University is headed by a subject representative, acting as research leader and responsible for the quality of education. The department's research develops knowledge about information systems' possibilities and limitations when it comes to supporting the way people work in, manage, and develop businesses. This research is typically conducted in collaboration with companies or governmental organizations. The department had substantial research experience in the area of information security, and information security management in particular. Altogether, this meant that the department had a network of stakeholders ready at hand when the development of the new master's program started.

2.2 Project Organization

The development of the new master's program was organized as a project. The overall project structure is shown in Fig. 1. The project team consisted of the project manager, the program manager, the head of department and course coordinators. The subject representative (the first author) acted as project manager. The project team consisted of the program manager (the third author), head of department and

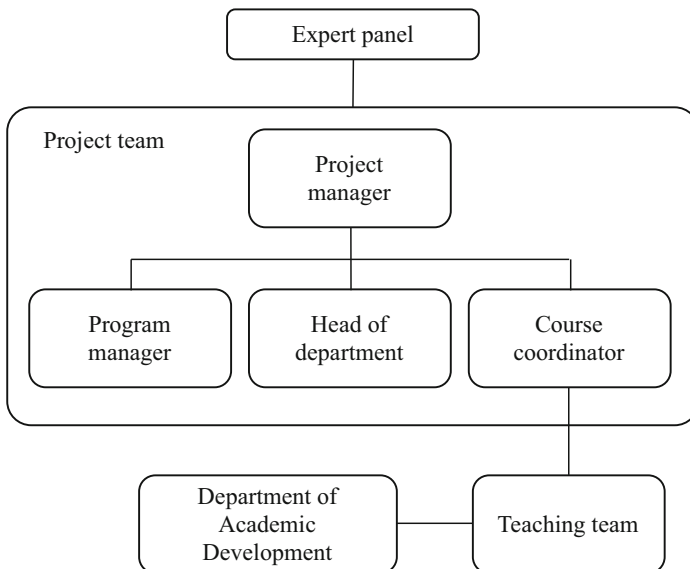


Fig. 1 Project organization

course coordinators (the second author acted as one of the course coordinators). The program manager had been assigned to this new master's program, being responsible for its launch and its administration once launched. The head of department was responsible for staffing of the new master's program and the needed competence development of staff. Finally, the course coordinators carried out development of courses together with teachers, forming teaching teams for each course.

An expert panel was formed consisting of the stakeholders and had an advisory role to the program manager and the project team. The expert panel included 13 stakeholders from public agencies, municipalities, and companies. In addition, the local student union organization attended all meetings with the expert panel. These stakeholders were selected from the department's existing collaboration partners (see Sect. 3.1 for details), and examples of stakeholder roles included are chief information security officer (CISO), consulting managers and information security consultants. The expert panel met twice per semester during the development work and continued to be active in giving advice and sharing insights also after the program was launched.

Finally, the project team received support from the university's Department for Academic Development. It offered advice and competence development for teachers on the two didactic models that were implemented in the program.

2.3 Didactic Model

When we started the development work, we decided that the new master's program should combine two didactic models: flipped classroom and case-based learning. In contemporary pedagogical research, the perspective of a student-centered and active learning process has gained attention as being more effective than traditional teaching. In flipped classroom, the focus is shifted from teachers' teaching to students' activities and motivation in learning. This means a move from the traditional lecture to more varied and active learning activities, chosen to inspire students to actively process the subject material (e.g. [10, 11]). The flipped classroom method allows for differentiated learning; giving students the opportunity to review course content at their own pace, as many times as they like, and so they can be better prepared for in-class activities.

The master's program is also anchored in case-based learning. Studies have shown that relevance is one of the most important aspects related to students' learning motivation [11]. Relevance can be established by using authentic, local and real-life examples and relating theory to practice [12]. Furthermore, case-based problems are well-suited to be combined with flipped classroom, as the focus can be placed on problem solving during physical classroom activities. The case-based problems are, in our case, planned in close collaboration with industry/governmental partners, i.e., our members of the expert panel. This means that the selected cases are based on the elicited requirements, which in turn drive the selection of theoretical parts/models that are applicable to introduce to the students.

3 Collecting Requirements Using the Delphi Method

Requirements are important to establish a foundation for any development process; developing a new master's program is no exception. Of course, the notion of requirement differs depending on the type of development work. We view a course requirement as a knowledge area in the master's program that one or more stakeholders need in order for the student to be employable.

Eliciting requirements is a challenging task, especially when several different stakeholders are involved. These stakeholders may have different or even conflicting requirements for the study program to be developed. Thus, "[t]here is no complete and well-defined set of requirements waiting to be discovered" [4]. Today, it is recognized that requirements are constructed through negotiation by stakeholders [5, 13, 14], and requirements elicitation can therefore be complex and time-consuming.

To deal with the negotiation aspects of requirements, we decided to elicit the course requirements using an adapted version of the Delphi method. This is a structured process often associated with an expert panel's opinion in forecasts studies [15], with the goal of arriving at a consensus on the subject discussed. The method was developed by RAND in the 1950s [8], to make forecasts in the US military. Over the years, it has been used in multiple disciplines (e.g., [16–19]); among these disciplines we find information systems (e.g., [20–23]). The method is considered to be a suitable investigation tool for topics for which the amount of available information is limited [24], and it has been suggested [25] and used [26] in the area of requirements engineering.

The Delphi method consists of several iterations of written questionnaires, in which the experts independently give their opinions or estimates. The answers the experts provide are anonymous. A facilitator collects the answers after each round of questionnaires, sorts the answers, and provides a summary report to each expert. Then the experts are given the option to re-think and adjust their own answer based on the summary report. After the experts answer each round of questionnaires, the facilitator collects all the answers and hands out a summary report of the answers to each expert. Then the experts review the summary report and either agree or disagree with the other experts' answers. The experts then fill out another questionnaire that gives them the opportunity to provide updated opinions based on what they understand from the summary report. The Delphi method is terminated when one or several of the following criteria are met: (1) a consensus on forecasts is achieved, (2) indications of experts' viewpoints are hardening and there are no signs towards consensus, or (3) experiencing expert fatigue [9, 27].

3.1 *Our Adapted Delphi Method*

It is important that the applied method fits the situation at hand, so we have therefore adapted our Delphi method based on knowledge from the field of situational method engineering [28]. Thus, our implementation should not be viewed as a textbox description of the Delphi method. We structured our Delphi method into four major steps: (1) populating the expert panel, (2) creating gross list of requirements, (3) iterations of requirements ranking, and (4) presenting the results.

Step 1: Populating the Expert Panel

To collect a relevant set of requirements we needed to populate our expert panel with practitioners, i.e., our stakeholders. Based on the idea that graduating students should be able to work in private and public organizations as well as act in the role as consultant, these were the main criteria for our selection of experts. Furthermore, the program has an explicit management perspective, which meant we searched for practitioners that could provide such input. We contacted practitioners in our existing research network and the final expert panel is presented in Table 1.

Step 2: Creating Gross List of Requirements

We started the requirements elicitation with an expert panel workshop. Thus, in this step we broke the anonymity of the expert panel. However, we deemed this workshop to be the most effective and efficient way to develop a gross list of requirements that could be used for the forthcoming negotiation of requirements. An alternative would have been to interview each of the experts or let the experts generate a gross list using an initial survey. However, the first alternative was deemed more resource-consuming compared to a workshop, and the second alternative was not deemed effective based on our previous experience from requirements engineering; generating initial requirements often requires communication about the overall goals

Table 1 The expert panel

Type of organization	Role
Private organization (product development)	CISO
Public organization (municipality)	CISO
Public organization (public agency)	CISO
Private organization (consultant)	Consult manager
Private organization (consultant)	Consult manager
Private organization (consultant)	Consult manager
Private organization (consultant)	Consult manager
Public organization (public agency)	Policy maker
Private organization (consultant)	Consultant manager in information security and law
Private organization (consultant)	Consult manager on information security standards
Private organization (consultant)	Consult manager on information security standards
Private organization (consultant)	Consultant in information security
Private organization (consultant)	Consultant in information security

of the development project. The workshop allowed us to introduce and discuss the overall goals of the master's program and how the requirement elicitation process was structured. In addition, we presented 10 broad themes under which we would structure the requirements. These themes had been derived from (a) requirements in the Swedish Higher Education Ordinance [29], and (b) benchmarking existing master's programs in Sweden and Europe. Thus, the reasons for not starting with a blank sheet were two-fold. First, there are certain teaching goals a master's program in Sweden must fulfil. Second, previous design knowledge, i.e., curriculums, of master's programs made it possible to position our new program in the existing context as well as, to some extent, build on others' designs. One advantage of choosing workshop as our way of working during this step was that ideas from one expert could trigger new requirements from other experts; thus, this could help build the gross list of requirements more effectively. All experts could contribute to requirements under each of the 10 broad themes by noting them on whiteboards (one for each theme). In total, we collected 193 requirements during this workshop.

The project manager and the program manager curated the collected data after this workshop, i.e., acting as the facilitators of the Delphi method. As facilitators, we analyzed the fit between the requirements and the themes, discussing how the requirements could be linked to the themes. The analysis was far from mechanical and involved subjective judgment. However, the analysis was necessary given the sheer number of collected requirements and that they had been phrased with very different granularity. As a result of this analysis, we both moved requirements between themes and categorized requirements. The latter became important to avoid ranking the same requirement multiple times. It was also important to group requirements together if there existed dependencies between them, i.e., treating them as one unit. For example, the detailed requirements "Reasonable cost for business", "External or internal education of employees is a matter of cost", "Investment", "The business should have the 'right' degree of security", "ROI", "Resources need to fit the business", "Business case", and "Cost-benefit" were categorized into the high-level requirement "Cost-benefit analysis". The detailed requirements were still kept, characterizing the description of the high-level requirements. The analysis resulted in our gross list of high-level requirements that we used for our first survey to the expert panel.

Step 3: Iterations of Ranking Requirements

We used a web-based survey tool to execute the ranking of requirements. It facilitated the communication with the expert panel. During each iteration the experts received lists of requirements to rank, one list for each theme. However, the design of the surveys differed between the iterations. During the first iteration, the experts anonymously ranked the requirements for importance and could comment on their rankings as well as provide comments on the requirement description as such. The latter was important for two reasons. First, it made it possible to develop additional requirements in areas where few requirements had been expressed. Second, it improved the descriptions of existing requirements; this would provide useful information during the forthcoming course design work, i.e., when

the requirements were implemented. Furthermore, because we prioritized eliciting additional requirements over ranking of existing requirements during this iteration, the experts only indicated the most important and the least important requirements. These numbers were summarized to determine the top and bottom requirements on our list of requirements list.

During the second iteration, the experts had the possibility to provide their final ranking of the requirements. We had used the provided comments on the requirement descriptions to rephrase the requirements. Every requirement was now described in a uniform manner. Each requirement started with either the phrase “Should have knowledge” or “Should have the ability to”, followed by a description of the requirement. Our above exemplified high-level requirement about “Cost-benefit” was rephrased as “Should have knowledge about assessing the financial consequences of investments in information security (ROI, Business case, cost-benefit)”. We only included six themes in the second ranking iteration. The included themes focused on courses that had information security content and themes that included requirements on research method, and master’s theses were excluded from the expert panel’s ranking. The data collected during the first iteration showed that the expert panel had difficulties providing requirements for the latter type of courses and rank ordering such requirements. Instead, the requirements on research method and master’s theses were dealt with separately by the faculty members (these requirements are therefore not covered in this chapter).

The ranking from the first iteration guided the order in which we presented the requirements in each theme during the second ranking iteration, i.e., showing the current ranked importance of each requirement. The experts anonymously ranked the requirements found in each of the six themes. During the second ranking, the expert panel had only the possibility to rank order the requirements. Thus, the experts could not comment on their rankings or provide any additional comments on the requirement description as such. Following Holeý, Feeley, Dixon and Whittaker [30] we used means and standard deviations for calculating the ranking position for the individual requirements. In addition, we calculated Kendall’s coefficient of concordance (aka Kendall’s W) to assess the consensus among the experts [9].

Step 4: Presenting the Results

We presented the final ranking of requirements at a workshop with the expert panel. The purpose was to present the requirements and how much of the course resources that the teaching team deemed necessary to implement the requirements. This meant presenting a first estimate of which requirements that would be implemented in the course design and with what depth. It meant discussing borderline requirements, i.e., both the possibility to include an additional requirement by adjusting how the course resources were used, and the necessity to remove a requirement. Furthermore, the teaching teams also discussed identified potential dependency relationships found in the way the requirements were ranked; issues that had not be acknowledged or fully understood before. The workshop resulted in a minor adjustment of the rankings, mostly resulting from solving the identified dependencies between requirements.

4 Illustrative Example – Social Aspects of Information Security

4.1 Program Overview

Örebro University's International Master's Program in Information Systems – Information Security Management comprises 120 credits distributed over 2 years. Based on the elicited requirements, the program provides in-depth studies within the information security management field and is comprised of both theoretical and practical elements. The program consists of 12 courses, derived from our 10 original themes. These 12 courses are briefly presented in Table 2, where the rightmost column shows whether the course was included in the first and second ranking iterations or not.

The first semester introduces the field and the three major types of information security controls, which are of technical, formal, and informal nature [31]. Technical controls, such as antivirus software and firewalls, are essential for organizations to stay protected. Still, such controls alone are not enough; organizations also need to implement formal controls, such as information security policies, to prevent information security breaches. Finally, informal controls focus on social aspects, such as employees' information security awareness and information security training programs. The second semester of the program focuses on ways in which an organization can apply a systematic approach to information security management.

The third and fourth semesters aim at allowing students to develop their knowledge of, and skills in, investigation work and research; providing them with the ability to identify and meet their need for knowledge; and allowing them to develop their ability to communicate the knowledge obtained and developed. Thus, these semesters are anchored in the faculty members' requirements for research work and requirements found in the Swedish Higher Education Ordinance [29] (these requirements are not covered in the chapter); the courses are presented here for the sake of completeness. Moreover, these two semesters aim at providing the students with an increased ability to reflect on research and investigation activities within the information systems field. The third and fourth semesters are important, not only for students who opt to pursue a doctoral degree, but also for those who, in different ways, would like to work with the management, development, or evaluation of information security.

Due to space limitations, it is not possible to present a complete account of all the elicited requirements across the different iterations, or how they have been prioritized and later used in the course design work. Below, we exemplify with the elicited and ranked requirements for the course Social Aspects of Information Security (7.5 credits) and how these requirements have been used in the design work. We also provide a brief account of the ranked requirements and the levels of consensus for all the courses that were included in the second ranking iteration.

Table 2 Program content

Course	Description	Semester	Included in ranking iteration	
			1st	2nd
Introduction to Information Security (7.5 credits)	The aim of this course is for the student to develop a basic understanding of information security and the central concepts and responsibilities within the field.	First	Yes	Yes
Regulatory Aspects of Information Security (7.5 credits)	The aim of this course is for the student to acquire knowledge about how information security is created by means of legislation, policies and regulations, and acquire abilities to craft policies.		Yes	Yes
Social Aspects of Information Security (7.5 credits)	The aim of this course is for the student to acquire knowledge about how employees' actions and mindset can contribute to information security.		Yes	Yes
Introduction to IT Security (7.5 credits)	The aim of this course is for the student to acquire knowledge of how software and hardware can be used to create information security.		Yes	Yes
Applied Information Security Management (12 credits)	The aim of this course is for the student to acquire knowledge about information security management system as a tool to safeguard operations being carried out in a way that is consistent with its identified goals.	Second	Yes	Yes
Setting Requirements for Information Security (7.5 credits)	The aim of this course is for the student to acquire abilities to communicate with clients about information security requirements in the development and procurement of information systems.		Yes	Yes
Information Security Management – Application Areas (10.5 credits)	The aim of this course is for the student to apply the knowledge they have obtained to a real-life information security problem.		Yes	No
Information Systems Theories (7.5 credits)	The aim of this course is for the student to acquire knowledge about theories used in the field of information systems and how they can be used as a tool for analysis or design in relation to information security.	Third	Yes	No
Qualitative Methods in Information Systems Research (7.5 credits)	The aim of this course is for the student to acquire knowledge about, and abilities to use, qualitative investigation methods.		Yes	No

(continued)

Table 2 (continued)

Course	Description	Semester	Included in ranking iteration	
			1st	2nd
Quantitative Methods in Information Systems Research (7.5 credits)	The aim of this course is for the student to acquire knowledge about, and abilities to use, quantitative investigation methods.		Yes	No
Professional and Academic Communication (7.5 credits)	The aim of this course is for the student to acquire knowledge about the communication of investigation results to both practitioners and researchers.		Yes	No
Thesis (30 credits)	The aim of this course is for the student to execute an independent investigation project.	Fourth	Yes	No

Table 3 Initial unranked requirements gathered during the workshop with the experts

High-level requirement	Detailed requirement
What guides human behavior	Rewards, incentives vs sanctions, commitment, motivation
Information security awareness	–
Culture	Attitudes – it does not happen to me
Tailored training	How can training programs target the needs of different roles? Workshops that are tailored to organizational needs

4.2 Social Aspects of Information Security – Elicited Requirements

The course Social Aspects of Information Security addresses informal measures [31] in information security work. The aim of this course is for the student to acquire knowledge about how employees' actions and mindset can contribute to information security.

Initial Requirements Workshop

During the initial requirements workshop with the experts, we elicited several requirements that were grouped to four high-level requirements, as shown in the leftmost column in Table 3. The experts stated that the course should address “What guides human behavior”, “Information security awareness”, “Culture”, and “Tailored training”. For some of these high-level requirements, we had also been able to elicit more detailed requirements that added descriptive characteristics (see the rightmost column in Table 3). However, in comparison to several of the other courses, we identified rather few requirements. Thus, developing additional requirements during the first Delphi iterations was important. The high-level requirements presented in Table 3 are unranked.

Table 4 First iteration of requirements and their ranking for the course Social Aspects of Information Security

Ranking	High-level requirement	Detailed requirement
Most important	Information security awareness	What is awareness about ^a
Less important	Culture	Attitudes – it does not happen to me, management culture, cultures among employees, culture models
Less important	Tailored training	How can training programs target the needs of different roles? Workshops that are tailored to organizational needs
Least important	What guides human behavior	Rewards, incentives vs sanctions, commitment, motivation, self-regulatory vs command-control ^a , risk ^a
New unranked	Different ways to raise information security awareness ^a	How to raise awareness ^a , raise security awareness ^a
New unranked	Social engineering ^a	Phishing ^a
New unranked	Ethical issues ^a	–
New unranked	Conflicting interests in organizations ^a	–

Note: ^aRequirements added after analyzing received comments during the first Delphi iteration. Newly added high-level requirements are unranked and therefore placed at the end of the table

First Delphi Iteration

The first Delphi iteration resulted in the experts ($n = 12$) providing a rough ranking, which is presented in Table 4. The ranking is shown in the leftmost column. The middle column contains the high-level requirement, and the rightmost column contains the detailed requirements for each high-level requirement. The experts were asked to stress the most important and the least important requirements, resulting in having knowledge about “Information security awareness” being ranked as the most important requirement. “What guides human behavior” was ranked as the least important requirement. More importantly, the existing list of requirements triggered the experts to express additional requirements using the survey’s free text fields. As a result, we were able to elicit four additional high-level requirements as well as several detailed requirements that could be added as details to these high-level requirements. The added high-level requirements are: “Different ways to raise information security awareness”, “Social engineering”, “Ethical issues”, and “Conflicting interest in organizations”. In Table 4, these new high-level requirements are unranked.

Second Delphi Iteration

Table 5 presents our final set of ranked high-level requirements, i.e., after the second Delphi iteration. The leftmost column presents the ranking number, the second column contains the requirement, the third column shows the calculated mean ranking score, and the rightmost shows the standard deviation. As discussed in Sect. 3.1, we reworked the requirements and expressed them using a uniformed format, starting with the phrase “Should have knowledge” or “Should have the ability to”, followed by a description of the requirements.

The first row shows that the experts ranked “Having knowledge about how to develop and design security awareness training to raise employees’ information security awareness” as the most important high-level requirement. Thus, this high-level requirement addresses “Information security awareness”, which was the most high-ranked requirement after the first Delphi iteration. However, there is a major difference between these requirements. Both address information security awareness, but the most high-ranked requirements in Table 5 shows more resemblance with the “Different ways to raise information security awareness” in Table 4. Thus, this shows the importance of the possibility to add requirements during the first Delphi iteration.

Table 5 Second iteration of requirements ranking for the course Social Aspects of Information Security

Ranking	Requirement	Mean	Standard deviation
1	Should have knowledge about how to develop and design security awareness training to raise employees’ information security awareness.	6.60	1.64
2	Should have knowledge about how to change people’s behaviors (e.g., different way of working, different perspectives).	6.00	2.11
3	Should have knowledge about information security culture (e.g., different models, different types of cultures such as management culture and cultures among employees).	5.30	1.88
4	Should have knowledge about what guides human behavior (e.g., risk apatite, loyalty, neutralization).	4.90	1.72
5	Should have knowledge about the consequences of low security awareness about threats (e.g., social engineering, phising, dumpster diving).	4.60	1.83
6	Should have knowledge about how to cultivate an information security culture.	4.40	1.71
7	Should have knowledge that there are several management systems in an organization and that may be conflicts between these systems because they are based on different values.	2.50	1.84
8	Should have knowledge about how to work with employees’ ethics, as many information security issues are related to ethical issues.	1.70	1.70

The calculated mean ranking values show clear differentiation between the high-level requirements. To assess the consensus among the experts ($n = 10$) during the second ranking iteration, Kendall's W statistic was calculated. For the ranking in Table 5, the Kendall's W is 0.46. This shows a moderate consensus on the ranking, and a fair confidence in ranks [9]. Furthermore, the standard deviations indicate that there is not much difference in dispersion between the individual high-level requirements. That being said, the highest degrees of agreements among the experts are found at both ends of the list, i.e., concerning the highest- and lowest-ranked high-level requirements. The greatest discrepancy, i.e., disagreement about the ranking position, is found in relation to the second high-level requirement.

4.3 Social Aspects of Information Security – Implementation of Requirements

The eight elicited high-level requirements presented in Table 5 were all addressed during the design of the course Social Aspects of Information Security. We used the ranking to decide which emphasis we should place on different course modules and in the exams. For example, as can be seen below, where we discuss course models, we place more emphasis on requirements 1 and 2 compared to requirement 8. The first two requirements play a key role in two modules, while requirement number 8 plays a minor role in one module. However, we did not use the ranking to decide in which order we should approach the different topics. It is sometimes beneficial to introduce topics in a certain order, because they build on each other (i.e., knowledge progression). Still, this order might differ from the ranking of the topics' relevance. The final course design included four main modules that implement flipped classroom and case-based learning. The content of these modules and how they relate to the requirements are discussed below.

The first module focuses on analyses of threats and incidents related to employees' information security behavior reported in media. This module is an implementation of requirement 5 in Table 5. During this module we introduce threats related to employees' information security behavior and their awareness of information security. These threats are introduced using one or more cases about real incidents that act as a catalyst for the students to search for additional cases in media. The students analyze these new cases to learn about how incidents can originate from threats such as phishing, human error, and theft. The students work in small groups and are examined with an oral presentation.

The second module focuses on theoretical models about social aspects that have an impact on employees' information security behavior. This module addresses requirements 3, 4, 7, and 8 in Table 5. The students read provided course literature, watch recorded lectures, and attend seminars where they receive cases to analyze and discuss. During these analyses they compare how different theoretical models can be used to explain the behavior in each case. The students study models that

explain employees' information security behavior using concepts, such as, appetite for risk, culture, ethics, punishment, neutralization, and values conflicts (e.g. [32–35]). We used the ranking to decide how much emphasis we should place on the different models. During the exam for this module, the students are provided with a case and must identify relevant social aspects that have guided employees' information security behavior.

The third module focuses on methods and tools to change employees' information security behavior. This module addresses requirements 1, 2, and 6 in Table 5. During this module the students read provided course literature and watch recorded lectures. The students also attend seminars where they analyze and discuss how different awareness raising programs fit existing organizational cultures in different cases. During this module, the students work with a case for which they are given the task of changing employees' information security behavior in an organization. The case work is a group assignment for which the students, based on the case details, must propose and argue for a way of working to change employees' information security behavior. In addition, their provided arguments need to be anchored in literature.

The fourth and final module is about assessing a chosen way of working to change employees' information security behavior. This module addresses requirements 1 and 2 in Table 5. At the end of the fourth module, each student hands in an individual assignment making an assessment of another group's case assignment from the third module. Thus, the student evaluates the method choices made and the arguments they are based on.

4.4 Overview of the Consensus on Ranked Requirements

As discussed in Sect. 3.1, only six courses (or themes¹) were included in the second Delphi iteration for which the experts rank ordered the high-level requirements. The calculated levels of consensus on the high-level requirements of each course are found in Table 6. As is seen in the second column from the left, the level of agreement among the experts differed between the courses. Following Schmidt [9] the levels of consensus among the experts range from weak agreement (0.3) to moderate agreement (0.5). The strongest consensus is found for the course Social Aspects of Information Security, while the weakest consensus is found for the course Introduction to Information Security.

Our further analysis of the data revealed an outlier. We identified one expert that rank ordered the requirements in a different way for all the courses. The fourth column therefore shows the calculated Kendall's W statistic with outliers removed.

¹ For these six themes there is a one-to-one relationship between the themes and the courses. We use word "course" and the names of the courses here because it is easier to refer to them in relation to the study program content presented in Table 2.

Table 6 Courses and consensus levels among the experts about the high-level requirements

Course	All		Outliers removed	
	Kendall's W	n	Kendall's W	n
Introduction to Information Security (7.5 credits)	0.23	9	0.29	8
Regulatory Aspects of Information Security (7.5 credits)	0.41	9	0.51	8
Social Aspects of Information Security (7.5 credits)	0.46	10	0.52	8
Introduction to IT Security (7.5 credits)	0.42	9	0.70	7
Applied Information Security Management (12 credits)	0.37	9	0.46	8
Setting Requirements for Information Security (7.5 credits)	0.37	10	0.46	8

For most courses, the rankings' recalculated levels of consensus reach moderate agreement (0.5) or even strong agreement (0.7). The strong agreement on the high-level requirements is found on the course Introduction to IT Security, where we removed two outliers. The course Introduction to Information Security is the one exception for which moderate agreement is not reached. After removing the outlier, the level of agreement is still close to weak agreement. Based on the Kendall's W statistics in the fourth columns and the fatigue in experts' participation [9, 27] we decided to halt the Delphi process after the second iteration.

4.5 Execution of Program Design

Enrollment Results

One major reason for the Informatics department at Örebro University to design and launch a new master's program was the low number of applicants to the existing program. When launching the new program, the goal was to enroll 15 students and consequently fill all study places. At the end of the old master's program, that had not been possible. Furthermore, this was viewed as a reasonable goal given that the new program was unknown to bachelor students in Sweden and internationally, and that in Sweden there has not been a strong tradition of applying to master's programs; at least, not in the field of information systems, where entry into the labor market is already very possible with a bachelor's degree.

Even though the program is an international master's program given in English, it seeks to admit both international and national students. As shown from the program design, it is not technocentric and focuses on the managerial aspects of information security. Hence, it aims to enroll students with backgrounds in informatics, information systems, computer science, and business administration. Table 7 shows the number of international and national applicants to the program since it was launched in 2018. The table also shows the number of enrolled students. As the numbers show, there has been a stable number of applicants to the master's program from the start and we already reached the goal of 15 enrolled students

Table 7 Number of applicants, enrolled students, and study places

	2018	2019	2020	2021
International applicants	148	119	139	19 ^a
National applicants	13	11	10	120 ^a
Enrolled students	15	14	23	26
Number of places	15	15	15	15

Note: ^aThere is significant difference in the number of applicants compared to 2020, which might be due to Covid 19. Enrolling in an international master's program was more problematic due to traveling restrictions. At the same time, the number of national applicants rose sharply, which might be due to uncertainties in the labor market

during the first year. Actually, during 2020 and 2021 we enrolled more students that was initially planned for the program.

Content Evaluation

If we return to our running example of the course Social Aspects of Information Security, the course evaluations show that the students have been satisfied with the course. For example, the first course evaluation from 2018 shows that 62.5% (n = 8) would recommend the course to other students, 12.5% would not recommend it, and 25% could not decide. The students had the possibility to provide free text answers and among the positive comments we found were: "Good teachers and interesting discussions", "I came to know that social mechanisms and information security policy has great role to change employees' information security behaviour" and "The teachers are knowledgeable, and the course material is relevant". Of course, these free text answers also included ideas for improvements. The most important comment addressed stress caused by the high number of group examinations during the course.

A formal alumni survey for this program is yet to be conducted. Nevertheless, we have kept track of the students that have graduated. For example, from the first batch, i.e., students enrolled in 2018, nine students have graduated so far. All these students are employed in areas that are relevant to their studies. The organizations that have employed these graduated students include consulting agencies, public agencies, the Swedish armed forces, and universities. When it comes to employment in the academic world, two students have decided to pursue a PhD degree and are enrolled as PhD students.

5 Lessons Learned

Above, we have given an account of the process of eliciting and prioritizing course requirements using an adapted Delphi method when designing a master's program in Information Systems with a specialization in information security management.

Regarding the adapted design of the method, some notable lessons can be learned from this case.

Using the Delphi method is a time- and cost-efficient way of obtaining rank ordered course requirements from an expert panel. The use of a digital survey tool made it possible to reach experts that were spread out geographically at a very low cost. In addition, compiling the results and creating a quantitative ranking was straightforward. A positive aspect for the experts was that they did not have to invest extensive time during the ranking iterations.

After our initial workshop and the first ranking iteration, it became clear that the experts had difficulties providing requirements and rank order requirements that were more research oriented, such as requirements about research methods and thesis writing. Of course, this is not related to the Delphi method as such but is due to many of the experts being unfamiliar with these topics. Their main area of competence is expertness in the subject area, in our case information security management. Thus, this challenge has more to do with how we have populated the expert panel. However, it is important to be aware of which types of requirements the experts will be able to rank order in a relevant way. It makes no sense to ask experts to rank order requirements that they are unfamiliar with.

It is important to pay attention to any outliers when assessing the experts' level of consensus regarding the ranking of course requirements. As is shown by our analysis of the levels of consensus among the experts about the high-level requirements, one of the experts consistently rank ordered requirements in a different way across all courses. The result of such analysis is important for deciding on when to terminate the Delphi process. Two criteria for termination are: (1) a strong consensus is reached among the experts, and (2) indications of experts' viewpoints are hardening or there are no signs towards consensus [9, 27]. In our case, removing the deviating expert's ranking showed that we moved towards stronger levels of consensus on almost all the courses included in the second ranking iteration. Furthermore, when comparing the details of the deviating expert's rankings with the other experts' ranking, it is doubtful that there would have been moves towards higher levels of agreements, as the difference were so large.

After the second ranking iteration we still had one course, Introduction to Information Security, for which the level of consensus among the experts was weak (see Table 6). Of course, when working with requirements, it is not a given that experts will agree. This is especially true when working with different stakeholders, because they can have conflicting interests [6, 7]. Thus, it is therefore important to assess whether the experts are representing different types of stakeholders. In our case, we had included experts from both private and public sectors, and both managers and consultants. However, the reached consensus levels for the other courses indicate that they constituted a fairly congruent stakeholder group. One possibility would have been to execute another round of ranking with the experts, including only the courses with weak or very weak consensus levels [9].

We experienced expert fatigue after two ranking iterations. Thus, if we had carried out a third iteration it would probably have made sense to focus on the courses with weak or very weak consensus levels. It would have been possible

to stress why another iteration was necessary for a subset of the courses, and hopefully boost participation among the experts. At the same time, we should also acknowledge that we carried out three activities together with the experts when including the expert panel workshop to create the gross list of requirements. If it had been possible to carry out this initial gathering of requirements in a more time-efficient way, this might have reduced expert fatigue during later ranking iterations. One technique used during Delphi-studies is that experts individually generates an initial list of topics to rank [9]. However, one should not underestimate the complexity in eliciting initial requirements, which is shown by the need to use our first Delphi iteration to refine the requirements at the same time as the experts carried out the first ranking. This shows the importance of starting the Delphi process with a set of well-formulated course requirements, which should not be confused with the rank ordering itself.

6 Conclusion and Advice

In this chapter, we have described the process of eliciting and prioritizing course requirements for an International Master's Program in Information Security Management, where we have used an adapted Delphi-method. We paid particular attention to how we have adapted the Delphi method to this particular task and provide an illustrative example from the design work for one of the courses in the master's program. The latter shows that the adaption was far from straightforward and included several challenges. Finally, we contribute with lessons learned from employing the Delphi method for this type of task.

The implications of our work are oriented to other teaching institutions that are developing or revising their teaching programs to increase practical relevance. Based on our application of the adapted Delphi method and our lessons learned, we provide the following advice for teaching institutions that intend to use the method:

- When populating the expert panel, it is important to include organizations that will employ the graduating students, i.e., the panel should be relevant. In addition, consider to what extent the potential panel members will actively participate in all the steps.
- Carefully create an initial idea of the study program and the competence areas needed. These competence areas are important guidance for the expert panel when the gross list of requirements is developed. When developing the gross list of requirements, consider if an initial joint workshop is a suitable option or if the experts individually should generate initial requirements lists. Take into consideration the resources available, the composition of the expert panel, and which alternative is most effective considering the culture at hand.
- Decide on which competence areas are suitable for elicitation of requirements from the expert panel. Focus on the areas that match the expert panel's main area

of competence. In case the study program includes parts in different competence areas, it might be worth considering more than one expert panel.

- Organize the requirements from the initial workshop into high-level requirements, using the low-level requirements as descriptions. Make sure that there are clear differences between the high-level requirements, and, if possible, no reciprocal relations between them. Structure the high-level requirements into a course structure before sending the first Delphi survey. The structure makes it clear how the requirements relate to each other and which requirements the experts are to rank order.
- Provide clear instructions to the expert panel on how to carry out the ranking. For example, it is important that the experts rank order all the requirements for a course and that they give the requirements different weights. The use of a digital survey tool can provide effective support in this area.
- When calculating levels of consensus on the high-level requirements, it is important to execute outlier analysis. It can provide important information about the reached consensus level and the need for additional ranking iterations. When deciding on another ranking iteration, it is also important to decide which courses should be included in the iteration. To lessen expert fatigue, only include courses where more information is needed.

References

1. ENISA: ENISA Threat Landscap 2021. European Union Agency For Cybersecurity (2021).
2. ENISA: ENISA Threat Landscape 2014. Overview of current and emerging cyber-threats. European Union Agency for Network and Information Security (2014).
3. ENISA: ENISA Threat Landscape Report 2018 – 15 Top Cyberthreats and Trends. European Union Agency For Cybersecurity (2018).
4. Boehm, B., Grunbacher, P., Briggs, R.O.: Developing groupware for requirements negotiation: lessons learned. *IEEE Software* 18(3), 46–55 (2001).
5. Kazman, R., In, H.P., Chen, H.-M.: From requirements negotiation to software architecture decisions. *Information and Software Technology* 47(8), 511–520 (2005).
6. Chabraborty, S., Sarkar, S., Sarkar, S.: An exploration into the process of requirements elicitation: a grounded approach. *Journal of the Association for Information Systems* 11(4), 212–249 (2010).
7. Holmström, J., Sawyer, S.: Requirements engineering blinders: exploring information systems developers' black-boxing of the emergent character of requirements. *European Journal of Information Systems* 20(1), 34–47 (2011).
8. Dalkey, N., Helmer, O.: An Experimental Application of the DELPHI Method to the Use of Experts. *Management Science* 9(3), 458–467 (1963).
9. Schmidt, R.C.: Managing Delphi Surveys Using Nonparametric Statistical Techniques. *Decision Sciences* 28(3), 763–774 (1997).
10. Marton, F., Säljö, R.: Kognitiv inriktning vid inläring. In: Marton, F., Hounsell, D., Entwistle, N. (eds.) *Hur lär vi*. Prisma, Stockholm, Sweden (2000).
11. Biggs, J., Tang, C.: *Teaching for Qualitative Learning at University*. Open University Press, Berkshire, England (2011).
12. Kember, D., Ho, A., Hong, C.: The importance of establishing relevance in motivating student learning. *Active Learning in Higher Education* 9(3), 249–263 (2008).

13. Seyff, N., Todoran, I., Caluser, K., Singer, L., Glinz, M.: Using popular social network sites to support requirements elicitation, prioritization and negotiation. *Journal of Internet Services and Applications* 6(1), 1–16 (2015).
14. Kotonya, G., Sommerville, I.: *Requirements engineering – processes and techniques*. John Wiley & Sons, New York, NY, USA (1998).
15. Rowe, G., Wright, G.: *Expert Opinions in Forecasting: Role of the Delphi Technique*. In: Armstrong, J.S. (ed.) *Principles of Forecasting: A Handbook of Researchers and Practitioners*, pp. 125–144. Kluwer Academic Publishers, Boston, MA (2001).
16. Guglyuvatyy, E., Stoianoff, N.P.: Applying the Delphi method as a research technique in tax law and policy. *Australian Tax Forum* 30(1), 179–204 (2015).
17. Hsiao, T.Y.: Establish standards of standard costing with the application of convergent gray zone test. *Eur J Oper Res* 168(2), 593–611 (2006).
18. Bokrantz, J., Skoogh, A., Berlin, C., Stahre, J.: Maintenance in digitalised manufacturing: Delphi-based scenarios for 2030. *International Journal of Production Economics* 191(September 2017), 154–169 (2017).
19. Jones, J., Hunter, D.: Qualitative research: Consensus methods for medical and health services research. *British Medical Journal* 311(7001), 376–380 (1995).
20. Brancheau, J.C., Janz, B.D., Wetherbe, J.C.: Key issues in information systems management: 1994–95 SIM Delphi results. *MIS Quarterly* 20(2), 225–242 (1996).
21. Holsapple, P., Joshi, K.: Knowledge manipulation activities: results of a Delphi study. *Information & Management* 39(6), 477–490 (2002).
22. Dhillon, G., Smith, K., Dissanayaka, I.: Information systems security research agenda: Exploring the gap between research and practice. *Journal of Strategic Information Systems* 30(4), Article number 101693 (2021).
23. Cata, T., Hackbarth, G.: Critical Success Factors for Electronic Therapy – A Delphi Study. *Communications of the Association for Information Systems* 34, Article 83 (2014).
24. Rowe, G., Wright, G., Bolger, F.: Delphi: A reevaluation of research and theory. *Technological Forecasting and Social Change* 39(3), 235–251 (1991).
25. Gutierrez, O.: *Expertmental Techniques for Information Requirements Analysis*. *Information & Management* 16(1), 31–43 (1989).
26. Triandini, E., Djunaidy, A., Siahaan, D.: Mapping Requirements into E-commerce Adoption Level: A Case Study Indonesia SMEs. 5th International Conference on Cyber and IT Service Management (CITSM 2017), pp. 1–5. IEEE, Denpasar, Indonesia (2017).
27. Worrell, J.L., Di Gangi, P.M., Bush, A.A.: Exploring the use of the Delphi method in accounting information systems research. *International Journal of Accounting Information Systems* 14(3), 193–208 (2013).
28. Henderson-Sellers, B., Ralyté, J., Ågerfalk, P.J., Rossi, M.: *Situational Method Engineering*. Springer-Verlag, Berlin Heidelberg (2014).
29. SFS 1993:100: Högskolefördordning. (1993).
30. Holey, E.A., Feeley, J.L., Dixon, J., Whittaker, V.J.: An exploration of the use of simple statistics to measure consensus and stability in Delphi studies. *BMC Medical Research Methodology* 7(52), 1–10 (2007).
31. Dhillon, G.: *Information Security – Text & Cases Prospect Press*, Burlington, USA (2017).
32. Siponen, M., Vance, A.: Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly* 34(3), 487–502 (2010).
33. Hedström, K., Kolkowska, E., Karlsson, F., Allen, J.P.: Value conflicts for information security management. *Journal of Strategic Information Systems* 20(4), 373–384 (2011).
34. Herath, T., Rao, H.: Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems* 18(2), 106–125 (2009).
35. Karlsson, M., Karlsson, F., Åström, J., Denk, T.: The effect of perceived organizational culture on employees' information security compliance. *Information & Computer Security Ahead-of-print(Ahead-of-print)*, (2021).

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



Rosanne English

1 Introduction

Cyber security is a key component of computing science degrees. Indeed many non-computing degrees now also incorporate cyber security as its prominence becomes increasingly more relevant and in demand [1]. For example, within the UK Northumbria University offers a Cybersecurity Law Masters programme [2], the University of Glasgow offers a [3] and the University of Portsmouth offers a Cybercrime Masters programme [4]. Each of these programmes are not offered by computing departments, though some do have modules within the programmes delivered by computing science departments.

University offerings such as those mentioned provide an opportunity to bridge the cyber security skills gap which has been estimated at 3.5 million unfilled cyber security jobs by 2025 [1]. More traditional offerings within generalised computing degrees are also increasing cyber security provision, particularly where accreditation requires it. For example, in the U.K. the British Computer Society increased their cyber security requirements in 2015 [5] However, delivery of cyber security in an academic environment also introduces a number of challenges.

One challenge is how such a module or programme should be taught. As noted by Schneider, some perceive the approach should be to teach the adversarial mindset through exploration of specific attacks, whilst others believe it should focus on the principals and concepts [6]. In the first approach, some students are able to generalise and develop the mindset such that they are then able to apply it to new contexts. However, others are less able to do so. As Schneider notes, those students who are by themselves unable to create an abstract mental model are

R. English (✉)
University of Strathclyde, Glasgow, Scotland
e-mail: Rosanne.English@strath.ac.uk

disadvantaged since they are unable to move with the fast-paced changes in cyber security. In contrast, using a more principal focused approach can result in students developing only a theoretical understanding and potential dissatisfaction due to lack of perceived ‘practicality’.

In order to better support students in understanding a combination of principles and practice to develop conceptual understanding as well as the adversarial mindset, a different approach to design might be helpful. This chapter will present a scenario-based approach to designing a cyber security module, which aims to help students understand principles as well as providing practice in applying these to different contexts.

2 How to Use this Chapter

It is anticipated that readers may approach this chapter with different goals in mind. In general you could fall into one of three categories;

1. You wish to gain an appreciation of scenario-based learning and how it may be applied to a security module design
2. You wish to develop a complete module which uses scenario-based learning as the key teaching technique
3. You wish to apply scenario-based learning to part of a module such as a single topic

Should you fall into the first category, it is suggested you approach this chapter by reading Sect. 3, which provides the background of scenario-based learning and presents the philosophy of why this could be helpful in a security module. You can then explore Sect. 4 which presents the design process and finish with the conclusion for a reflection on the delivery of this approach.

Should you fall into the second category, it is suggested that you may skip Sect. 3 on the philosophy of this approach and the background and instead focus on Sect. 4 which introduces the design process of this case study. The hope is that having read the design approach, one can consider how this may be applied in one’s own context. Having done so, you can then consider the reflection on delivery of the module which is presented in Sect. 5. Section 5 is split into three aspects; structure, facilitating sessions, and assessment. Structure and facilitation aim to provide insight into the practicalities of delivery of such a module, whilst assessment provides a reflection on the types of assessment one may consider. As such, if one has their own assessment already in mind, this aspect can be missed.

Should you fall into the third category, you may wish to consider Sect. 3 if you are trying to determine why one might wish to use SBL. You could then read Sect. 4 which addresses the design, though if applying to a single topic you should bear this in mind as the case study discusses a module as a whole. In Sect. 5 on delivery, you may wish to focus more on the Facilitating Sessions element as this is applicable to a smaller set, whilst overall structure and assessment may be less helpful.

3 Bridging the Gap Between Theory and Application: Considering Learning Models for Cyber Security

In determining how to bridge the gap between theory and practice approaches to teaching cyber security, we can look to constructive learning design which focuses on students actively constructing their knowledge and understanding through authentic tasks which have clear objectives [7]. Constructivism is well established within computing science education [8] and its guiding principle is that students learn through experience, and connect learning to prior experiences to build mental schemas [9]. Using a constructivist technique applied to cyber security provides an appropriate learning model lens to design a module through.

Advocates of constructivism emphasise seven key goals for constructivist learning [10]. Each goal is considered below, with a reflection on how they align with the objective of teaching cyber security in a way which bridges principles and practice.

1. **Experience should be combined with knowledge construction** This goal aligns with the aim of combining the two general approaches to teaching cyber security as proposed by Schneider [6].
2. **Experience and appreciation of multiple viewpoints** This goal emphasises how there are often multiple acceptable solutions or perspectives for any given problem within a context. Honebein argues that it is important for learners to be able to consider a range of alternative solutions and engage in evaluating and testing the most appropriate solution instead of fixating on one correct solution [10]. This is especially important in cyber security, e.g. in encryption there are multiple ciphers and the best solution can depend on the context.
3. **Embed learning in realistic contexts:** This goal supports the need to ensure the learning context is relevant and realistic. In 1991 Lave and Wegner [11] introduced the concept of situational learning, which describes this goal. Situational learning can be thought of as learning which happens within the appropriate context. Lave and Wegner argue that situational learning is essential for acquisition of professional skills and that one cannot and should not remove the context from the learning process. The reasoning is that without context, concepts are taught in isolation and this limits a learner's ability to adapt to different contexts. This is of particular importance in cyber security where it is critical that learners are able to apply understanding of core concepts, such as encryption and network security, to new situations and thus bridge the gap between theory and application. Learning concepts entirely independent of context is sub-optimal as it would introduce a challenge for a learner to transition to applying these in the real world.
4. **Promote student ownership of learning:** this aims to ensure students engage and take responsibility for their learning over passive consumption of knowledge sometimes referred to as shallow learning. To be able to combine principles and practice this is important aim. Biggs [12] argues that more active learning activities encourages deep learning.

5. **Immerse learning in a social space:** this emphasises the benefit of learning within a social space, e.g. through group discussions.
6. **Encode learning in multiple formats:** This relates to a variety of formats for learning materials to support learners in being able to learn from various sources.
7. **Develop student metacognition and reflexive practice:** Metacognition can be thought of as an individual's understanding and regulation of their learning. Developing metacognition is a key factor in helping learners develop the skills to work in a rapidly changing environment such as cyber security. Consequently, it is important to choose a learning model with this in mind to ensure learners are well scaffolded to understand cyber security. Volet [13] conducted experiments which showed that metacognition and learning outcomes were improved both in the short and long term where content-relevant metacognition strategies were modelled and a socially supportive learning environment was employed. As a result, a learning model which allows adaption to the context of cyber security is important.

Having now established constructivism as an appropriate guiding principle, we can now consider how this model can be implemented through active learning techniques. In order to ensure realistic contexts and immersion in social spaces, In 1991 Lave and Wegner [11] introduced the concept of situational learning, which can be thought of as learning which happens within the appropriate context. They argue that situational learning is essential for acquisition of professional skills and that one cannot and should not remove the context from the learning process. The reasoning is that without context, concepts are taught in isolation and this limits a learner's ability to adapt to different contexts.

3.1 Problem-Based Learning

One pedagogical model which aligns with constructivist and situational learning is problem-based learning (PBL). In a problem-based learning design, students are placed into small groups and are given a problem which they must explore and present a solution for. A tutor is provided for each group to act as a guide, ensuring students stay on task and assisting where necessary.

Problem-based learning has been considered in regards to cyber security for similar reasons to those outlined in this chapter. For example, the work by Shivapurkar [14] and the Cyber Security Knowledge Exchange project [15].

Shivapurkar et al. use the structure of Maastricht University on problem-based learning [14] to demonstrate how this could be applied to cyber security education. In their paper the authors present two scenarios. The first scenario asks students to consider how they could execute phishing attacks, requiring students to identify what phishing attacks are and the practicalities of trying to implement such an attack. The second problem focuses on an attack on a Windows SMB port which allows the attacker to steal a file, and asks students to determine how such an attack

could be executed as well as which techniques they could use to stop such an attack. However, the paper indicates that applying this within a course had not yet taken place.

Unfortunately the AdvanceHE project website appears to be no longer maintained, thus it was not possible to access the resources or develop an understanding of how it was achieved. However, reviewing the presentation from the AdvanceHE website shows that the motivation behind the project was similar, in that the intention was to help students develop the skills of evaluating a system on the basis of its security.

The PBL model is typically used as the primary mode of teaching throughout a given module, and tends to make use of larger more complex problems with multiple sources of information for learners. Learners in PBL also need to set their own learning objectives and identify areas they need to learn before being able to tackle the problem [16].

Barrows [17] identified six characteristics of PBL as follows:

1. Learner centred
2. Small student groups supported by tutor
3. Tutor acts as a facilitator
4. Problems should be authentic
5. Problems should be designed such that learners must develop the required knowledge and skills to solve them
6. New knowledge should be acquired through self-directed learning

As class sizes grow, it is unlikely that resources would be available to ensure that characteristics 2 and 3 are met. Similarly, it can be difficult to structure self-directed learning with increasingly diverse cohorts. Developing more complex problems with multiple information sources can also be challenging for a single educator to implement for a complete course.

This can be seen in the work by Moust et al. who reviewed the practical implementation of the Maastricht University PBL approach [18]. The authors note a demise in the seven step process for implementing PBL which was established along with the University approximately 30 years prior. For example, they observed students were less likely to perform self-directed learning and literature searches, and student-staff ratios were not sufficiently adequate as to allow this approach. Consequently an alternative approach was considered.

3.2 Scenario-Based Learning

Scenario-based learning was identified as a constructivist approach similar to problem-based learning which still helps bridge the gap between theory and practice whilst providing more scalability to combat the challenges of implementing PBL.

A scenario-based approach provides students with problem scenarios which they have to explore and present solutions to.

Scenario-Based Learning often focuses on written scenarios as the primary source and is not the only method used within teaching. It is also more flexible which means it can be adapted for larger class sizes with less resource, whilst also ensuring students get sufficient scaffolding to support a diverse cohort of learners.

Similarities between SBL and PBL include the need for a realistic scenario, which has elements which are not clearly defined to mimic the uncertainty of the real world [16].

Scenario-Based learning is a technique which aligns with situational learning by provision of context through scenarios. It provides learners a real world style context in which they apply their knowledge and skills. The technique can help students engage with the material due to the connection with an authentic context [19].

Scenario-Based Learning can have a number of positive effects on the student learning journey. It can improve student motivation, critical thinking, and problem-solving[27]. Such an approach helps shift learners from a knowledge-based exploration of cyber security to higher cognitive skills [20]. As a result, scenario-based learning suits itself well to cyber security as a field.

Whilst there is little on how to approach the design and development of a cyber module which uses the scenario or problem-based approach, there is some literature around designing such modules for other subjects. Notably, Wolfe presents the design of a database security module with a single scenario as the focus for exploring database security [21]. In particular the following elements are identified:

- Place the student into the narrative
- Base the scenario on a real situation
- Use small businesses rather than large
- Incorporate realistic defects
- Simplify business circumstances

Firstly, placing the student into the narrative of the scenario gives the student a role to play in the situation [21]. Aspects for consideration in this role are the objective of the role, what they can and cannot do (e.g. levels of authority). Another key element is authenticity. Wolfe describes this as ‘realism’ of the scenario. This could be achieved in a number of ways, such as simplification of a larger problem seen in the real world either experienced personally, experienced by colleagues or friends, and examples from the news.

The size of the scenario, whilst trying to be realistic, is necessarily limited in complexity. This is due to the time and resource available for a given module or teaching session. One element to consider here is the size of the business used in a scenario. As argued by Wolfe [21], the complexity of larger organisations would pose too much of a challenge for students to meaningfully explore in the limited time frame of a module. This is particularly important if a scenario is only used for exploration of one topic. As a result, smaller businesses or more contained scenarios allow a sufficiently authentic problem without overwhelming students.

Also related to authenticity is the need to incorporate realistic defects. The aim of a security module is to help learners understand the kinds of security vulnerabilities

and identify corresponding mitigation techniques. By modelling realistic defects, this provides learners the opportunity to assess a given context in terms of security. However, once more one needs to be careful that there are not so many issues such that it might overwhelm the learners.

Summarising these attributes for developing security scenarios, the following criteria for developing security scenarios are proposed:

- Authenticity with limitations
- Incorporate realistic defects
- Simplify business circumstances

Having decided on an appropriate technique and identified criteria for developing cyber security scenarios, the next step is to explore how this can be applied to the design of a cyber security module. This is addressed in the next section which presents a case study covering the design of a cyber security model.

4 Designing a Scenario-Based Cyber Security Module

This section outlines the approach taken in designing the curriculum of a scenario-based cyber security module. The module is a UK based final honours year cyber security fundamentals module. It starts by considering the intended learning objectives (ILOs) and corresponding content, then the development of scenarios followed by the delivery structure.

The proposed procedure for development of scenarios is a 6 step process as follows:

1. Identify module ILOs related to this task
2. Identify related tasks necessary to achieve ILO(s) from step 1
3. Identify appropriate contexts, e.g. small medical practice
4. Write the scenario incorporating the tasks and context from steps 2 and 3
5. Ensure the scenario is appropriate and revise as necessary
6. Develop assessment

These steps will be covered in detail in the remainder of this section.

4.1 Learning Outcomes and Identifying Tasks

In identifying a suitable structure and content for the module, it is recommended to use a constructive alignment approach. As noted by Biggs [12], this approach requires the setting of intended learning outcomes prior to teaching and designing learning activities which give learners the opportunity to engage with that task. In this application, the scenario-based questions are the primary learning activities.

In developing the intended learning outcomes for a module it can be helpful to use the cognitive domain Bloom's taxonomy [22] or the revised taxonomy

[23] to ensure the objectives are set at an appropriate level. Bloom's taxonomy allows the level appropriate verbs to include in the intended learning outcomes. For example, evaluation would typically be expected in hours years as well as in Masters programmes. Thus if exploring a range of cryptography protocols, evaluation of an appropriate protocol to apply in a given situation would be more suitable at higher levels than exploring the knowledge levels like explain the TLS protocol. However, it should be noted that in order to demonstrate higher levels of achievement, it is necessary to work through the lower levels related to knowledge and understanding.

The following learning outcomes are those for a foundational cyber security module which covers core concepts of cryptography and secure communication, network security, and user authentication and access control.

- Differentiate between secure communication information security solutions to determine an appropriate solution for a given context
- Evaluate an existing or proposed system in terms of potential security vulnerabilities and recommend the most appropriate security solution to apply
- Critique the security of a given network scenario and propose appropriate mitigation techniques
- Perform to analysis of cyber risk and threat modelling

Having now identified learning outcomes, the next step is to identify the content which allows those objectives to be achieved. This constructive alignment approach throughout the design process ensures students are scaffolded in being able to achieve these objectives.

Table 1 is a proposed structure for an introductory cyber security module which aligns with the ILOs above and prioritises the key concepts of cryptography, authentication and access control, and network security as the core areas which allow exploration of other fields such as web security and human aspects of security. This design is intended as a 10 week module, however this is extensible to cover a longer period (e.g. a 20 week module could provide additional depth or additional topics). The design could also be reduced for a shorter module, e.g. 5 weeks focusing on the key areas of cryptography, access control and network security.

More generally, a scenario-based approach can be applied to a range of security module types. For example, in a pen testing module the scenarios would be relating to vulnerabilities in systems and approaches to attacking the system using those vulnerabilities. This chapter focuses on an introductory secure systems approach, but it would also work well for a module which explores things from a cyber management and governance perspective. For example, student could be provided with scenarios and asked to explore which cyber framework might work best, or they could be asked to complete a risk assessment for a given scenario. The approach is very flexible, and could encompass a wide range of areas of cyber security.

It is now possible to break down each topic into further content elements. For example, which specific cryptographic protocols are to be covered etc. Having such a breakdown then permits the lecturer to decide an appropriate range of material to support students in achieving the ILOs.

Table 1 Overview of topics

Week	Topic	Sample subtopics
1	Principles of cyber security	CIA triad, important terminology, related legislation
2	Cryptography	Cryptography primitives such as cryptographic hashes, components and overview of encryption
3	Cryptography	Further cryptography e.g. PK infrastructure and digital signatures
4	Authentication and access control	Authentication factors, access control models, biometric authentication, secure password management
5	Network security attacks	Attacks such as machine in the middle, replay attacks and denial of service
6	Network security defence	Defence mechanisms e.g. firewalls, demilitarised zones, VPNs and TLS
7	Malware	Structure and mitigation
8	Web security	OWASP top 10 and mitigation techniques
9	Cyber risk management	Stages of risk management
10	Human-centred security	Phishing, social engineering

The content can then be the basis of developed comprehension materials such as lectures, videos, reading etc. Note that a mix of media can be helpful to keep learners engaged.

Having now determined the appropriate ILOs and corresponding content, the next step is to develop scenarios which allow learners the chance to practice skills which demonstrate the ILOs.

4.2 Identifying Context and Developing Scenarios

Having determined the ILOs and topics, one can then consider the components a student must understand in order to be able to engage fully with a scenario.

For example, let us consider the following learning objective- “differentiate between secure communication information security solutions to determine an appropriate solution for a given context”. This objective can be further broken into the following tasks:

- understanding of components of modern ciphers and how they are used in different ciphers
- compare and contrast different ciphers for different purposes
- evaluate a scenario to determine the most appropriate cryptographic solution

A related scenario then must ensure an opportunity to demonstrate understanding of cryptography primitives and their use in ciphers, compare different ciphers, and justify a choice been different ciphers for the given scenario.

Having identified the ILOs and related task breakdown, the next step is to identify an appropriate context. The following are some examples of contexts:

- a small software development business (helpful when looking at technical elements)
- a medical practice (helpful when exploring access to particularly sensitive data)
- a friend seeking advice e.g. on aspects of cryptography to ensure security of their data (helpful in ensuring comprehension)

Of course, there are many more possible contexts. It can be helpful to keep up to date with recent cyber attacks which can provide inspiration for the context. For example, the Wannacry ransomware attack could be abstracted into an example of software not being updated and malware exploiting a vulnerability in non-patched software. Students could be asked to consider the mitigation techniques which may have prevented this, in particular more substantial procedures may have mitigated the issue of some branches not updating software with a known vulnerability. This is a helpful example to highlight that technical controls are not the only option, an element which can be overlooked by students with a penchant for technical solutions.

We will continue with the example cryptography example where we identified tasks as; demonstrate understanding of cryptography primitives and their use in ciphers, compare different ciphers, and justify a choice been different ciphers for the given scenario. The context we will use will be a friend seeking advice.

Having now selected a context, the scenario can be written to incorporate the tasks with the context. A scenario could then be:

A friend is building a dynamic website for their local sports club of which they are a board member. Information on members of the club must be stored securely in a database. Your friend is confident in developing the code and interface, but is unsure of the best choices in regards to data security. In particular, they wish to use a block cipher but do not know how to differentiate between a block cipher and a stream cipher. As your friend is aware of your experience in cyber security they have asked for your help.

1. Your friend asks you to explain the difference between block and stream ciphers, and why you may chose one over another
2. Having clarified this, your friend is now aware of two block ciphers—AES and Blowfish. They wish to understand the distinction in the mechanisms used within these ciphers, and whether they should chose one over the other for storing sensitive data which is not passwords. Provide a comparison of the ciphers along with an evaluation as to whether one cipher would be more suitable for this context over the other.

Recall it is helpful to place the learner into the narrative, in this instance the learner is being asked for help. We can also ensure all elements of the tasks have been covered, the task is realistic (indeed the author was asked to complete a similar task) and circumstances have been simplified as there is no mention of GDPR or

Table 2 A proforma structure for a scenario-based activity design

Element	Description
Module ILOs:	The ILOs for the module as they relate to this scenario-based activity
Key skills:	The breakdown of skills which allow the above ILO(s) to be demonstrated
Scenario context:	The narrative of the scenario.
Questions	Specific prompts and questions for learners to answer

consideration of how the data is gathered, as well as consideration of physical security storage.

Other examples can include those such as the Wannacry example, which is authentic with a realistic defect and business circumstances can be simplified by lack of consideration of the connection and different approaches between different areas or branches. In terms of incorporating the student into such a scenario, they could be employed as a security consultant to explore what led to the incident and how to mitigate against a similar issue in the future. To ensure consistency and clarity, a proposed proforma which provides the structure of a scenario-based activity is provided in Table 2.

4.3 Assessment

The assessment should allow students to apply skills developed through completion of the SBL exercises. For example, one form of assessment would be a scenario-based written exam. This is an exam where the questions are structured in the same format as the scenario-based questions throughout the module. However, it should be more constrained than those used in facilitated sessions as questions and scenarios which are too open can overwhelm students within an exam setting. An overly open question can also mean learners struggle to interpret what is being asked, and consequently answers may be more varied than is optimal.

If using an exam, it is worth considering making it an open book exam where students can reference their notes. The reasoning is that it reduces the need for students to perform rote memorisation and instead focuses on the comprehension of concepts and being able to perform the skills required by the ILOs. However, this can introduce issues with academic integrity, as such it is worth reminding learners of expected standards.

A sample exam question context is provided as follows. You have a friend who has set up their small business computer network and are working to secure it. They do not understand much about network security and have asked for your help. On their network they have a file server which they wish to be able to access from outside their business network.

A corresponding question could then be “Propose and justify a firewall structure which would allow your friend to access their server from the internet but would not expose the local address of the server.”

It is also possible to make use of coursework which makes use of the scenarios. For example, a case study analysis could be an appropriate coursework. In such an assessment, learners would be asked to identify (or pick from a select list) a recent security incident and analyse what went wrong, and what mitigation strategies might be suitable for the given context. This also has the benefit of providing learners with an opportunity to refine their communication skills.

Coursework can also use a scenario which provides the context for the assignment. For example, learners are asked to imagine they are part of a red or blue team and they have been tasked with assessing the security of a given system and then to report their findings. This approach has the benefit of a balance between hands on activities and reflective evaluation.

The scope of the scenario for assessment can also be scaled depending on the module duration and time available. For example, it is possible to develop a larger scale scenario with multiple facets which provide the basis for all tutorial questions and discussions across the module. Such a scenario would likely emulate real world scenarios more closely, and could bring together a range of incidents relating to the different topics within the module. Such a scenario may focus on a fictional company, with a defined network structure, digital assets and authentication policies as well as information security policies. The scenario information could be built up over time, depending on the area being covered at any given time within the module.

Another approach to managing scope would be to consider a jigsaw style approach [24], where the components are split between different groups within the class and each group reports on their element. For example, if an assessment was to analyse a security data set which has a range of possible issues or attacks which can be considered, then groups could be allocated a specific subset of the data or a more focused goal. The groups could then be combined to provide an overall review of the security data provided.

There are likely many more options which accommodate this style, but hopefully the few examples above provide inspiration as to what might be possible. We have now addressed how one can approach designing scenario-based activities. The next element to consider is how these activities combine into a delivery approach for the module as a whole. This is addressed in the next section where a series of steps to designing a scenario-based cyber module are provided with a breakdown of each step.

5 Delivery

At this stage, one should now have a clear overview of the module ILOs, the content, and the scenarios and corresponding tasks as well as assessment. The next step is to put this together into a structure for delivery. This section aims to address this,

providing insight into some of the challenges and logistics of delivery. This is split into three areas; structure, facilitating SBL sessions, and assessment.

5.1 Structure

By incorporating scenario-based learning one might anticipate the required contact hours would increase. If traditional content delivery (e.g. through didactic lectures) is maintained then this would be the case, as the lecturer should be on hand to facilitate learner explorations of scenarios. However, a more appropriate approach would be to use the flipped classroom model for delivery. This is one way to ensure the content is delivered to students whilst making space for the content checking and scenario engagement essential for scenario based learning to take place.

Baker [25] coins the term flipping the classroom as an instructional model where the content element (the traditional lecture) is removed from the in class time. Learners are expected to engage with the content prior to attending class. The reasoning being that meaningful application of concepts and techniques can then take place with the instructor on hand to be the “guide on the side” [26]. The content of the module can take the format of pre-recorded lecture videos, or reading or other activities. The key element is that students must engage with the material prior to the sessions with the lecturer to ensure they get the most of the interactive elements.

The structure of a typical week is then as shown in Fig 1. From Fig 1 one can see that the lecturer should ensure material which requires students to engage with it prior to a facilitated session should be made available sufficiently far in advance. Giving learners as much time as you can to process the content is ideal, as is setting a consistent day to release such content. One approach could be that material for a given week is release on the Monday in the week prior. This provides students with at least 1 week to engage with the content.

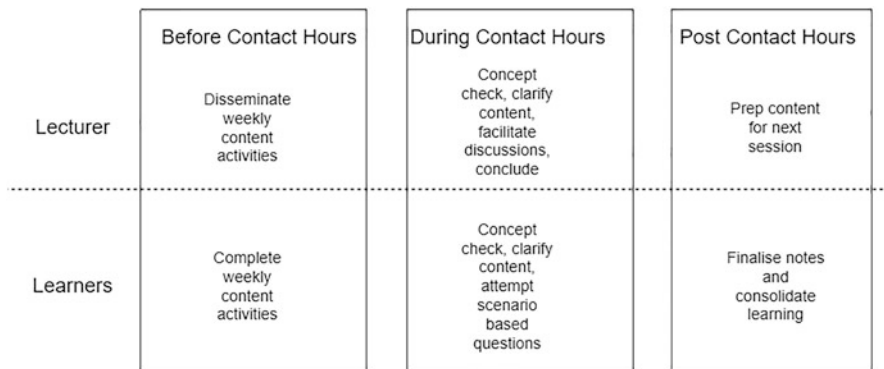


Fig. 1 A typical week structure for scenario-based flipped delivery

You may also wish to have activities which students can complete in order to concept check. This helps students identify misunderstandings prior to engaging with the scenarios. There are a range of options including activities such as multiple choice (which has the benefit of automated marking and feedback) or minute papers, or if class time permits then a more traditional tutorial which checks fundamental comprehension and application of module content material. It is helpful for the lecturer to be able to identify any common areas of confusion and directly address these either asynchronously through the Virtual Learning Environment (or other communication channel) or whilst in a class session which allows for a conversation with learners to take place. The key is that prior to engaging with the scenario-based activities, the learner should have had the opportunity to explore the related content. The lecturer should make clear to learners how the typical week works, including tasks per week and when they should engage with them. It can also be helpful to present the reasoning behind the approach, as well as giving students an opportunity to ask questions about the structure or how to complete activities they may not be familiar with. Since this is important to set expectations, it is recommended this is covered in the first contact hour with students. This means in the first week one would not expect students to have completed any engagement activities prior to attending. However, in the following weeks students should become more comfortable with the consistent structure.

Aspects the lecturer may also wish to highlight in the initial session is how long content activities should take on average per week, any other expected behaviour such as taking notes, how to get clarification on module content, and an overview of the learning objectives, weekly content and tasks, and assessment structure and deadlines.

It is important to note that using a different mode of delivery can be challenging. In particular, a number of students feel uncomfortable with this approach as it is unfamiliar. Due to the nature of the structure, there are also areas for which there is no single acceptable answer. This can also be unfamiliar for students who may be more comfortable with coding exercises where there is less room for interpretation.

To aim to address these aspects, it is important to clearly define the structure and reasoning for the format of the module. It may be necessary to repeat this multiple times, and provide reassurance to learners that well reasoned answers are acceptable. This is of particular importance for summative assessment such as exams, where learners are more likely expect a single answer is the only solution, it is helpful to clarify that this is not true. It can also be helpful to encourage learners to speak with you directly to discuss their answers if they are unclear.

Another obstacle is the need for more self-directed learning, which can be challenging for learners who struggle to motivate themselves to engage with module content prior to SBL sessions. One option to increase motivation is to include low stakes continuous assessment, such as multiple choice quizzes. Alternatively, regular prompts and a clear list of actions required week by week can help students manage their studies more effectively.

Having decided the overall structure of the module, the next aspect to address is the facilitation of scenario-based activity sessions.

5.2 *Facilitating Sessions*

As this method is similar to a problem-based learning structure, sessions should be structured in a way which allows students to break into teams to discuss a scenario. If this is online, this can be through breakout groups. If it is in person, then depending on the room this may be more challenging, but is still possible. Sufficiently clear instructions on group choice should be provided, and it may be helpful to maintain the same groups for each week or change depending on the cohort. For example, the author's experience for undergraduate honours students is that they prefer to chose their own group, whilst Masters students typically prefer to be allocated as they have yet to make friends. A third alternative is that those who wish to chose can do so, but those who don't can abstain and be randomly allocated to a group at a defined deadline.

One challenge to facilitation is class size. This approach is generally easier to complete with a smaller class size as the lecturer can ensure all teams receive guidance during the session. This is harder with larger class sizes, e.g. a class of 100 in a 50 min session using teams of 5 would mean the lecturer would only have 2.5 min per team. Clearly this is sub-optimal, thus a number of adjustments are necessary to accommodate larger class sizes. To adapt, time at the start should be provided to allow students to clarify any material they may be unsure of. This means time is not required for moving around teams providing the same content clarification.

Students can also be made responsible for reporting back from these discussions. Such accountability, as noted by Duch et al. [16], gives students stronger motivation for engaging with the discussion. Groups could then be randomly chosen to report their solutions, or alternatively teams can place these in a shared document. Students are often reluctant to volunteer solutions independently when in a class setting, so it is recommended a mechanism other than simply asking the class what they achieved is used.

Guidance provided in the scenario-based activities should also be more explicit for larger class sizes. For example, a more open scenario-based activity could be broken down into smaller component parts. This would also allow the class to discuss this at each stage, rather than a single discussion at the end which may result in disengagement when given longer to discuss. Duch recommends students are given no more than 15 min to discuss when part of a larger class [16].

Below is an example of a scenario developed to explore user authentication. A hospital emergency department decides to digitise their patient records. Currently patient records are paper-based, and staff carry them around the hospital as necessary. The problem is that records are being left in rooms with patients, who can clearly see them. Also, records are being lost and are not always returned to the main storage cabinet. This means in emergency situations medical staff are unable to access the records as quickly as they need to.

The current proposal is to place a computer device in each of the common areas (such as the waiting room and reception desk), as well as in each of the cubicles

where patients are dealt with. The staff who need to access the records include administrators (who check patients in), nurses, and doctors. An authentication mechanism needs to be selected for the devices. Consider each of the following questions, and propose a solution given an unlimited budget. You might need to do some research to address all questions. The prompts or questions which go along with this scenario can have more or less structure depending on the size of the class. For example, below are the prompts which could be used with a smaller class size.

- Consider the positives and negatives of different user authentication methods for this scenario and present a proposed solution with appropriate justification.

Compare this with the prompts for a larger class as shown below.

- What should you consider when selecting an authentication mechanism for this scenario? What might the requirements be?
- What options are available for authentication?
- How does each option match your requirements?
- Given your answers to the previous questions, which option would you choose and why?
- Assume now that you have a smaller budget, what impact would this have on your choice?

Note that in the first set students are given a more open question since the lecturer can support students by giving the breakdown if needed. However, in the second set this is broken down into smaller parts to guide students since the lecturer will not be able to provide as much support to all teams. This allows the lecturer to incorporate check points where if a small number of teams are struggling, it is possible to directly address this to the whole class.

During the session, the facilitator can move between as many groups as possible within the time. It is important to try not to spend a disproportionate time with a single group. If dealing with a larger class, it may be helpful to address common issues to the class as a whole instead of repeating across multiple groups. This can be achieved in a number of ways, e.g. through a broadcast message functionality if online, or by calling the class together before splitting into groups once more.

One challenge which may occur is groups not engaging with the discussion. Depending on the year of the cohort, it may be helpful to allow learners to self select groups. By doing so, they are more likely to work with peers they are comfortable with which can help discussion. The lecturer can also prompt learners with specific questions, or ask what support they need. Of course, there is only so much one can do and so if learners do not wish to engage it may simply be helpful to explain the reasoning behind the approach and move on to another group. Should common misunderstandings or queries arise through such discussions it can be helpful to note these for reporting to the whole class.

Having completed the allocated time for discussion, it is important to bring the class back together to summarise the results. To ensure students are on track, it can be helpful to summarise possible solutions. Ideally these would be delivered by the learners themselves, however it can be challenging to get learners to volunteer

solutions. To combat this, the session could be structured such that groups are randomly selected, or a schedule for each team to present solutions could be used.

There can be challenges in delivery of such a session. Depending on the stage and background of learners, some may have less practice in skills such as communication. If this is the case, it can be helpful to provide a range of sources such as links to the relevant university skills support team as well as general resources on skills such as web resources. In aiding learners in consolidating their learning after the session, a temporary summary of the discussions could be provided. This also helps support learners who may have missed a session, or who may have a different first language. The summary could be written, or audio, or a combination of audio and visual. The temporary nature is suggested as a way to help learners engage consistently throughout the module.

5.3 Assessment

Delivery of assessment with the scenario-based learning structure is similar to normal delivery, however if the assessment uses a scenario then it can be helpful to discuss an example in a session. For instance if an assessment involves completing penetration testing and a reflective video presentation for a defined client, it can be helpful to show examples and discuss as a class what was done well and what could be improved. This can help learners understand how a marking rubric can be applied to the final product.

If using an exam which asks scenario-based questions, it can be helpful to provide an example of an exam question. As discussed previously, by design the scenario-based questions in an unseen written exam are generally more precise. Also, as the questions have marks allocated to them it can be helpful to give students an opportunity to see how marks are distributed. For example, it is common for learners to focus more on the definitions and to neglect the context. This means a lower level of attainment as the structure is specifically designed to assess application of theory to a novel context. As such it can be helpful to highlight a ‘strong’ response indicating where marks are earned and the importance of application to the given context.

For learners with English as a second or further language, this can also be a cause for stress. Learners can struggle with the combination of terminology as well as the language for contexts. To support learners with this challenge, it can be helpful to build a glossary of both terminology as well as the types of context used.

Having covered the approach to designing and running a module which uses SBL as a mode of delivery, it is important to consider some of the challenges which have arisen in the author’s experience. Firstly, it is common that a number of students feel uncomfortable with this approach as it is unfamiliar. Due to the nature of the structure, there are also areas for which there is no single acceptable answer. This can also be unfamiliar for students.

To aim to address these aspects, it is important to clearly define the structure and reasoning for the format of the module. It may be necessary to repeat this multiple times, and provide reassurance to learners that well reasoned answers are acceptable. In particular for exams, where learners are more likely expect a single answer is the only solution, it is helpful to clarify that this is not true. It can also be helpful to encourage learners to speak with you directly to discuss their answers if they are unclear.

Another challenge is the need for more self-directed learning, which can be challenging for learners who struggle to motivate themselves to engage with module content prior to SBL sessions. One option to increase motivation is to include small continuous assessment, such as low stakes multiple choice quizzes. Alternatively, regular prompts and a clear list of actions required week by week.

6 Conclusion

Throughout this chapter we have explored scenario-based learning as one approach to help bridge the gap between theory and application of cyber security to unknown contexts. A case study was presented to illustrate how one can design and implement a cyber security module using this approach. We have also discussed some of the challenges which can arise in the delivery of such a module, including learners discomfort with a new approach and ensuring engagement for optimal performance.

It is helpful to remember that although this chapter represents the process for a complete module design, elements of scenario-based learning can be implemented in much smaller way. For example, taking a particular topic which lends itself to this and applying SBL for that topic. It can also be built up over time, e.g. incrementally applying to a variety of topics until an appropriate level is reached. The hope is that as the reader you are now aware of the possibilities, and may decide to implement this in your own security modules, even in a small way.

References

1. Cybersecurity Ventures (2021), Cybersecurity Jobs Report, <https://cybersecurityventures.com/jobs/>
2. Cyber Law Masters, Northumbria University, Accessed March 2022, <https://www.northumbria.ac.uk/study-at-northumbria/courses/master-of-laws-law-cyber-law-newcastle-dtflcb6/>
3. Global Security Masters, University of Glasgow, Accessed March 2022, <https://www.gla.ac.uk/postgraduate/taught/globalsecurity/>
4. Cybercrime Masters, University of Portsmouth, Accessed March 2022, <https://www.port.ac.uk/study/courses/msc-cybercrime#careers-and-opportunities>
5. Tom Crick, James H. Davenport, Alastair Irons, and Tom Prickett. 2019. A UK Case Study on Cybersecurity Education and Accreditation. In 2019 IEEE Frontiers in Education Conference (FIE). IEEE Press, 1–9. <https://doi.org/10.1109/FIE43999.2019.9028407>
6. F. B. Schneider, "Cybersecurity Education in Universities," in IEEE Security & Privacy, vol. 11, no. 4, pp. 3–4, July-Aug. 2013, <https://doi.org/10.1109/MSP.2013.84>

7. Bada, S. O. (2015). Constructivism Learning Theory: A Paradigm for Teaching and Learning. *Journal of Research & Method in Education*, 5, 66–70.
8. Ben-Ari, M. Constructivism in computer science education. *SIGCSE Bulletin* (Association for Computing Machinery, Special Interest Group on Computer Science Education), 30(1), 257–261, 1998, <https://doi.org/10.1145/274790.274308>
9. Gagnon, George W., and Collay, Michelle, *Constructivist Learning Design: Key Questions for Teaching to Standards*. United States, SAGE Publications, 2005.
10. Honebein, Peter C. “Seven goals for the design of constructivist learning environments.” *Constructivist learning environments: Case studies in instructional design* (1996): 11–24.
11. Lave, J., Wenger, E. (1991). *Situated Learning: Legitimate Peripheral Participation* (Learning in Doing: Social, Cognitive and Computational Perspectives). Cambridge: Cambridge University Press. <https://doi.org/10.1017/CBO9780511815355>
12. What the student does: teaching for enhanced learning, John Biggs, 1999, *Higher Education Research & Development*, 18(1), 57–75
13. Simone E. Volet, Modelling and coaching of relevant metacognitive strategies for enhancing university students’ learning, *Learning and Instruction*, Volume 1, Issue 4, 1991, Pages 319–336, ISSN 0959-4752, [https://doi.org/10.1016/0959-4752\(91\)90012-W](https://doi.org/10.1016/0959-4752(91)90012-W).
14. Shivapurkar, Mandar, Sajal Bhatia, and Irfan Ahmed. “Problem-based Learning for Cybersecurity Education.” In *Journal of The Colloquium for Information Systems Security Education*, vol. 7, no. 1, pp. 6–6. 2020.
15. The Cyber Security Knowledge Exchange project, Edge Hill University, <https://www.cyberedge.uk/cske/index.php>. Accessed March 2022
16. Duch, B. J., Groh, S. E., & Allen, D. E. (Eds.). (2001). *The power of problem-based learning*. Sterling, VA: Stylus
17. Barrows, H. S. Problem-based learning in medicine and beyond: A brief overview. In Wilkerson, L., Gijsselaers, W. H. (Eds.), *Bring problem-based learning to higher education: Theory and practice* (pp. 3–12). San Francisco: Jossey-Bass, 1996
18. Moust, J. H. C., Van Berkel, H. J. M., & Schmidt, H. G. (2005). Signs of erosion: Reflections on three decades of problem-based learning at Maastricht University. *Higher Education*, 50(4), 665–683. <https://doi.org/10.1007/s10734-004-6371-z>
19. Mio, Cristina and Ventura-Medina, Esther and Joao, Elsa (2019) Scenario-based eLearning to promote active learning in large cohorts -Students’ perspective. *Computer Applications in Engineering Education* , 27 (4). pp. 894–909. ISSN 1099-0542. <https://doi.org/10.1002/cae.22123>
20. Dolog, P., Thomsen, L. L., & Thomsen, B. (2016). Assessing problem-based learning in a software engineering curriculum using Bloom’s Taxonomy and the IEEE software engineering body of knowledge. *ACM Transactions on Computing Education*, 16(3), 1–41. <https://doi.org/10.1145/2845091>
21. Wolfe, A. D. Using a Business Compromise Scenario to Teach Cybersecurity, *Innovations in Cybersecurity Education*, 157–177, https://doi.org/10.1007/978-3-030-50244-7_9
22. Bloom, B. S., Englehart, M. D., Furst, E. J., Hill, W. H., & Krathwohl, D. R. (1956). *The Taxonomy of educational objectives, handbook I: The Cognitive domain*. New York: David McKay Co., Inc.
23. Anderson, Lorin W., David R. Krathwohl, and Benjamin S. Bloom. *A Taxonomy for Learning, Teaching, and Assessing : A Revision of Bloom’s Taxonomy of Educational Objectives*. Abridged ed. 2001
24. Aronson, E. and Patnoe, S. (1997) *The Jigsaw Classroom*, 2nd edn, Longman, New York
25. Baker, J. W. 2000. The “classroom flip”: Using web course management tools to become the guide by the side. 11th International Conference on College Teaching and Learning, Jacksonville, FL.
26. King, Alison. “From Sage on the Stage to Guide on the Side.” *College Teaching*, vol. 41, no. 1, Taylor & Francis, Ltd., 1993, pp. 30–35, <http://www.jstor.org/stable/27558571>
27. S. Naidu, M. Menon, C. Gunawardena, D. Lekamge, S. Karaunanayaka (2007). How Scenario-Based Learning Can Engender Reflective Practice in Distance Education in Finding online voice: Stories Told by Experienced Online Educators, Chapter 4

Enabling Teamwork in Cybersecurity Courses



Joanne L. Hall and Asha Rao

1 Introduction

The socio-technical nature of cybersecurity [49] makes working in a team essential, leading to teamwork becoming increasingly sought after by the industry [24]. Teams could be led by a manager or arise when working freelance with clients and/or suppliers. Thus, preparing cybersecurity students to be job-ready requires educators to design learning experiences that develop teamwork skills across the course of study. In this paper, we discuss the measures taken within the Master of Cyber Security at RMIT University to build this much-needed skill among students.

Teamwork is a non-technical skill needed for enhanced graduate employability [53], with Dawson and Thomson [19] (2018), arguing that the complexity of the cyber domain requires a unique combination of skills, ranging from domain-specific knowledge, to technical and non-technical skills, including teamwork, for success. A recent survey indicates cybersecurity recruiters in Australia seek evidence of teamwork skills within their junior recruits [24].

While development of teamwork skills is a requirement for accreditation in many professionally accredited degrees including Engineering [4] and Nursing [42], the cybersecurity profession continues to be neither accredited nor licensed. One pathway to employment in the cybersecurity industry is via highly regarded industry certifications offered by industry bodies such as ISACA [3] and (ISC)² [32]. However, teamwork skills are neither assessed nor developed in the exam-based assessments of these industry certifications.

J. L. Hall · A. Rao (✉)
RMIT University, Melbourne, VIC, Australia
e-mail: joanne.hall@rmit.edu.au; asha.rao@rmit.edu.au

Furthermore, in the case of the CISSP [31] certification, for example, a prerequisite for accreditation is 5 years of experience in a cybersecurity domain, meaning a recent graduate of a higher education degree is unlikely to be accredited.

Educational institutions need to take responsibility for understanding the needs of employers and tailoring their courses of study to fit. Reflecting on the ongoing debate (see, for example, [16]) about the inability of Higher Education institutions to deliver graduates with the skills needed by employers, Succi and Canovi [53] look at the increased relevance of non-technical skills and the dichotomy of what employability means to students versus employers. Employer groups and higher education institutions need to work in tandem with both students and recent graduates, who must understand their responsibility in developing the skills needed by industry [53].

In higher education in general, a common way of developing teamwork skills in university students is by assigning team-based tasks. However, as research shows, the resulting experience does not always prepare job-ready graduates [12, 20, 53]. Given the dichotomy between the expectations of employers and students [53], it is possible that such teams are actually just groups of students working together on a task. This could be especially true in the area of cybersecurity [19, 46], which consists of complex tasks requiring participants with different domain knowledge and experience to work together. Rajivan et al. in their paper on cyber defence teams [46], define a *functioning* team (vs. a group) as a group with members from diverse backgrounds working in an *interdependent* manner.

In this paper, we describe the various measures used within the cybersecurity master's degree at RMIT to enable teams to function as envisaged by industry. The rest of the paper is organised as follows: in the rest of this section, we give details of the RMIT Master of Cyber Security, which forms the basis of our case study. In Sect. 2, we discuss the existing literature on teamwork in STEM fields, including the value of teamwork in the cybersecurity field, and the challenges that exist in designing teamwork in higher education. Section 3 details the different existing frameworks proposed to enable a functioning team, while Sect. 4 presents current good practices to support the development of teamwork skills. Section 5 gives the different ways teamwork is managed in the different courses within the RMIT University Master of Cyber Security degree, while in Sect. 6, we discuss our findings. Finally, we give the conclusion and some recommendations.

1.1 RMIT University Master of Cyber Security

The RMIT University Master of Cyber Security¹ is a 2-year program aimed at providing an in-depth study of the mathematical, technical, and business aspects of information security. Although the title of the program uses the current *buzz*

¹ <http://www1.rmit.edu.au/handbook/mc159p18auscy>.

word, cybersecurity, the aim of the program, since its inception in 2000, has been to provide graduates with a comprehensive understanding of the socio-technical nature of information security.

The word cybersecurity came into local parlance about a decade ago. It has since become a buzz word. On the other hand, information security has a much longer history, with the UK Department of Trade and Industry publishing a code of practice for Information Security governance² in 1992. Cybersecurity is a subset of information security [59]: information security is the protection of information everywhere, whereas cybersecurity is restricted to the preservation of information in cyberspace. This is an important difference. The RMIT Master of Cyber Security aims to provide students with in-depth knowledge of protecting information in all states: online and off.

The program learning outcomes (PLOs) of the RMIT Master of Cyber Security degree include

- International orientation and strategic thinking,
- Critical analysis and problem solving,
- Communication,
- Ethical values,
- Self-management, teamwork, and leadership.

Each of these PLOs are expanded in terms of cyber and information security. The courses (=subjects) include assessment of ‘work practices’ within real or simulated workplace settings, and feedback from industry experts.

The masters degree consists of 16 courses, with eight core courses and eight electives. The first four core courses include the fundamental courses in discrete mathematics and programming, as well as an introductory course in information security, coupled with Case Studies in Cyber Security. The learning activities of Case Studies in Cyber Security are mostly seminars delivered by industry experts and aimed at informing students of the breadth of roles present in the field. The remaining core courses are Cryptography for Cyber Security, Information Systems Risk Management, and two project courses: Industry Awareness Project and Industry Linkage Project. In the capstone course, Industry Linkage Project, students work on a team project with an industry mentor, or as an intern within an industry mentor’s organisation.

The electives in the program range from cybersecurity specific to broader business, IT, and mathematical skills. The cybersecurity specific elective courses include Ethical Hacking, Information Theory for Secure Communications, Multi-factor Authentication, Frontiers of Applied Cryptography, and Cloud Security. Students can take IT electives such as Systems Architecture, business electives such as Digital Strategy, and mathematics electives such as Applied Analytics. The electives enable students to tailor their degree keeping in mind their undergraduate qualifications, their prior work experience, and their career goals.

² <https://www.pc-history.org/17799.htm>.

The PLO Self-management, Teamwork and Leadership includes the detail “work autonomously and effectively within and potentially as a leader of an interdisciplinary team”. With this PLO in mind, teamwork has been built into four of the core courses: Case studies in Cyber Security, Information Systems Risk Management, and the capstone sequence Industry Awareness Project, and Industry Linkage Project. These four courses are distributed across the 2 years of the program, allowing students to build teamwork skills as they progress in their studies. Further details of the teamwork in the different courses are given in Sect. 5.

2 Literature Review on Teamwork in STEM

There is a myth [15] of the solo scientist working in their own lab to understand the natural world, or the solo engineer in their workshop inventing world-changing technology. Science, Technology, Engineering, and Mathematics (STEM) are, and have always been, highly collaborative [15]. Roald Amundsen did not explore the South Pole alone, he had an expedition team. Florence Nightingale did not revolutionise healthcare by herself, she worked with other medical and military staff. An individual may lead a project; they work with a team to implement the project.

Most job advertisements for technical positions, including in engineering, IT, and cybersecurity, now require applicants to have certain non-technical skills. This requirement can be traced back a couple of decades. The globalisation of the workforce led to increased outsourcing [5] and off-shoring of jobs, resulting in technical professionals moving up the value chain. These technical professionals are, therefore, required to demonstrate a broader range of skills.

Teamwork is one of the non-technical skills listed as a requirement for technical roles. While Thompson does not explicitly list teamwork in his book, *People Skills* [56], he talks about collaboration and teamwork being valuable for effective time management. He notes the need for setting clear parameters and role expectations, as these help in reducing confusion and conflict [56].

With the increasing listing of teamwork as a required skill in job advertisements, many STEM degrees and courses now include teamwork skills as part of program and course outcomes. These teamwork skills are usually developed by including team-based tasks and assessments. Such team-based tasks can be short classroom exercises or longer projects lasting the entire teaching period. Teams can be pairs, small teams of 3–4 students, or larger teams of up to 8 students. Teams can be self-selecting, randomly allocated, or allocated according to some plan.

It is common for students to complain about team-based assessments, with high performing students feeling their grades have been or will be impacted by team members not sharing their academic skills, motivation, availability, or behavioural norms [47]. Research [14] shows that when a group did not perform well, the students who scored less were given harsher peer reviews. Thus, this perception of disadvantage could result in non-functioning or low-functioning teams.

Ability and life situations will often differ within the diverse cohort of students in any class. While some students aim to excel in every class and have both the ability and life situation to do so, every cohort will possibly contain capable students facing barriers due to life circumstances [52]. Examples of such circumstances include health, family expectations, paid work arrangements, insecure housing, English as a second language, sexism, and racism. A team-based assessment could negatively impact the learning experience of such diverse groups. Even when team members have prior knowledge of each other, varying expectations may still exist. All in all, teamwork, when not designed well, could become a burden rather than a learning experience.

2.1 *The Value of Teamwork in a Cybersecurity Career*

A number of researchers have looked at the value of teamwork within a cybersecurity career—based on what recruiters have been looking for over the past couple of decades.

In 2019, Peslak and Hunsinger [43] analysed almost 500 job ads in the area of cybersecurity as well as searching for definitions of cybersecurity. Their research showed that cybersecurity was very much a technical field in both aspects, with recruiters looking mainly for general technical skills, with some looking for a variety of specific skills that were by no means uniform.

While non-technical skills or soft skills are not mentioned in [43], other research shows the increasing value of these skills within the cybersecurity industry. Way back in 2006, Hentea and Dhillon [27] noted that information security and assurance was not a computer science sub-set and should include technical and non-technical aspects. Non-technical skills are now definitely considered important for a successful cybersecurity professional, with a number of papers [19, 24, 25] explicitly listing teamwork and the need to work in multi-disciplinary teams as an essential part of securing information systems. A recent survey of Australian cybersecurity recruiters found that many employers look for teamwork skills in their recruits [24].

It is important to clarify the definition of teamwork that we use in this paper. A group of people working together on the same project, does not always indicate a *functioning team* [46]. A group may complete a large task by allocating sub-tasks to each member of the group to complete independently. A functioning team, on the other hand, has members who work interdependently with no sub-task completed in isolation.

As tasks get more complex, the likelihood of the sub-tasks being highly interdependent increases, resulting in a greater need for the team to function as a whole to achieve the desired outcome. The need for functioning teams [35] in cybersecurity is only set to increase, given the socio-technical nature of cybersecurity, increased online presence due to COVID-19 and lockdowns, reliance on the ever more devices being added to the Internet of things, as well as the resultant increase in cross-border

cyber crime. Hence, it is necessary to enable functioning teams within cybersecurity programs of study.

2.2 Challenges of Teamwork Tasks in Higher Education

Team assessment is often the most common complaint in student course surveys [63]. Student's negative experiences include cultural clashes between team members, social loafing, the impact on the whole team of an individual's illness, and perception of unclear or unfair awarding of grades. We detail each of these below.

2.2.1 Cultural Clash of Team Members

A diverse range of perspectives within a team can lead to better solutions [36]. However, the more highly diverse a team, the more time and structure needed by the team to arrive at good solutions [7]. Student projects have a typical duration of less than a teaching semester (10–12 weeks), and student teams have to function as a team, rather than a group, right from the beginning for optimal project success. This is a difficult proposition in reality, especially if the course is at the beginning of the program of study.

Another aspect of cultural clash relates to the culture within a particular area. Male dominated disciplines traditionally have masculine behavioural norms. Such behavioural norms can result in challenges for students (and/or teaching staff) either not familiar or unable/unwilling to adhere to such norms. This is particularly true within regards to teamwork and team-based assessments [57]. Given that both the cybersecurity industry as well as cybersecurity education cohorts are male dominated [33], gender is an important factor that must be considered.

In a number of controlled studies, diverse teams were found to perform more objectively in examining evidence and making choices than homogeneous teams [48]. Many organisations are now recognising the value of diversity and including formal diversity practices in their talent management practices [38]. Providing students with opportunities to work in diverse teams can assist in their transition to the workforce.

2.2.2 Social Loafing

Another common complaint by students is regarding team members who don't 'pull their weight'. Known as social loafing, or 'free riding', this is the practice of some individuals to contribute less to a team project than their team mates [23]. The assumption among social loafers often seems to be that since others will probably do enough to achieve a satisfactory outcome, they do not need to engage as much.

Most students believe that some amount of social loafing has occurred in their team. The four aspects of social loafing [50] include not being available (for meetings, submitting work on time, etc.), submitting work of poor quality that then needs rework by team mates, being preoccupied with technology, such as during team meetings, and not contributing to discussions.

Social loafing could be considered the opposite of conscientiousness, the desire to do every task well. A high degree of conscientiousness is highly correlated with project success [7]. Better performing teams have lower incidence of social loafing among team members [23]. Hence, strategies for monitoring social loafing behaviours and early intervention need to be designed into team assessments [44].

2.2.3 Unexpected Illness or Withdrawal of a Team Member

Unexpected events [55], such as illness of a team member, can lead to extra pressure on teams, as it results in conflicting demands. On the one hand, the team member experiencing the illness needs the sympathy of their team mates. On the other hand, the team has to adapt quickly to the changing situation, re-allocating work, and adjusting deadlines etc. An added possible venue of disruption is the withdrawal of a team member from the course. In Australia, students are able to withdraw without financial penalty before the ‘census’ date. This census date is sometimes 6 weeks after the start of semester. This can cause the same level of disruption as an unexpected illness, although of a slightly different variety.

With teamwork becoming a requirement in industry, building teams that adapt to unexpected, disruptive events is necessary. The continuing COVID pandemic has only accelerated the need for such adaptation [62].

2.2.4 Grades Unclear or Improperly Assigned

While students understand the need for teamwork, they are often reluctant to engage in teamwork in higher education. A major concern for students is not getting the requisite acknowledgment of their work in a group assessment [63]. The view that they know how much work is needed but their team mates may not, often underwrites this perception. Student teams, particularly those with culturally diverse team members, benefit from structured assistance to communicate effectively, work collaboratively, and manage their projects [6].

Teamwork is usually assessed for the team as a whole with a group grade. However, a collective group grade is often seen as unfair by students [37] and possibly undermining of their ability to maintain their individuality in group assessments. Thus, there needs to be individual accountability built into the design of teamwork [41].

All of the above challenges to teamwork need to be addressed if we are to enable students to learn from their teamwork experience. In the next section, we look at some existing frameworks being used to enable functioning teams.

3 Enabling Functioning Teams: Existing Frameworks

Given the importance of teamwork in cybersecurity [2], it is important to explicitly develop teamwork skills within a graduate course of study, rather than assuming students will just pick it up. From a growth mindset [21] teamwork skills can be learnt, and team-based assessments could provide the ideal setting. However, just providing students with multiple opportunities to develop teamwork skills is insufficient [63].

As educators, we need to plan and design experiences, providing learning opportunities as well as reinforcing successful teamwork skills. Curriculum needs to be designed to scaffold teamwork skills across a course of study. In this section, we describe existing frameworks to develop teamwork skills among students.

3.1 *Team Charters*

A team charter is a tool used to support the success of team-based projects and is widely used in industry [18, 30, 51]. A variety of disciplines including business [29, 34, 55], engineering [28, 39] and nursing [58] use team charters. With regard to students, team charters can aid in the development of teamwork skills across a variety of courses.

A good team charter provides a framework for each team member to self-assess and understand other team members' skills and motivations at the beginning of a project [40]. This, then, provides a pathway to a more productive and inclusive environment. A team charter supports the setting up of a shared understanding of expectations within the team. Devoting time at the start of a project to construct a team charter is likely to result in a well-functioning team with Mathieu and Rapp [40] finding a correlation between the quality of a team's charter and sustained team performance.

Including a statement about respectful behaviour in their team charter ensures each student is cognisant of the behaviours expected of them [54], thereby reducing some of the friction from cultural clashes. A higher level of satisfaction with team-based assessments is evident when each team member's contribution is clearly stated [34]. Thus, a team charter with a well-thought out plan at the start of a project provides a framework for better team cohesion and for acknowledging each team member's contribution. Courtright et al. [18] show that team charters especially enhance the performance of teams with less conscientious members.

Requiring each team to write (and submit) their own team charter, along with a weekly plan, at the beginning of a team project sets both behavioral and technical work expectations, encourages reflective learning, and is useful evidence when assigning grades. Johnson et al. [34] found that teams with charters reported higher conflict levels, but these, however, did not negatively impact either peer evaluations

or output quality. Thus, developing and submitting the team charter and weekly plan gives students' ownership of their contributions and behaviour, thereby reducing the incidence of dissatisfied teams. A quality team charter can uplift the performance of a mediocre team [1, 18]. Having clear expectations and consequences agreed at the beginning of the project means less energy is spent on resolving conflicts, leading to better technical output [55].

Teams benefit from explicit initial discussions about project tasks, behavioural norms, time commitment, and work quality. Although, often, students do not initially see the point of a formal team charter, those that experience even minor obstacles in their teamwork report the value they see in the formally documented team charter as a tool for conflict resolution [54].

3.2 Project Management Practices

While a team charter is a useful tool to support a successful team project [30], detailed record keeping across the project timeline with interim submissions, further supports students in the management of their team assessment tasks.

Record keeping of all team meetings, decisions, plans, tasks allocated and completed along with timelines for the same, all contribute to the effective management of a project. In addition, these activities provide important evidence of each team member's contribution.

Regular logging of contributions leads to uneven contributions becoming noticeable. Such logging of contributions is more realistic than the case reported in Burdett [10] where students were required to "declare, ... all students contributed equally ...". Evidence suggests that in 99% of cases, the workload is equidistributed. However, the majority of students perceive some level of social loafing [63], but are often unwilling to directly report on their peers. Indirect reporting of social loafing becomes possible when students record contributions with sufficient detail that an uneven contribution is noticeable by teaching staff.

Interim submissions as touch points, allow for formal feedback on the team's progress, as well as providing a formal opportunity to report social loafing. These interim submissions also enable the teaching team to understand the difficulties a team, or the cohort as a whole, may be having in understanding a semester-long project's guidelines. Furthermore, interim submissions also 'chunk' a larger project, thereby reducing the sense of being overwhelmed that some students experience with large assessment tasks. Thus, interim submissions can help with student perceptions of a manageable workload, which is correlated with student satisfaction [44].

3.3 Constructive Alignment of Assessment Criteria

Successful teamwork management in a university course is enabled by appropriate assessment criteria. If teamwork is a course learning outcome, then the learning activities should be designed to teach teamwork skills, with assessments designed to explicitly assess the teamwork [8]. If assessment criteria only focus on technical project outcomes, then teamwork is not being assessed.

Constructively aligning assessment tasks with the learning outcomes [47] supports students' understanding of the process of learning. Assessment criteria explicitly valuing teamwork can motivate students to work as a team. Care must be taken in the description of the assessment tasks and the assessment criteria: ambiguous assessment instructions (including criteria) can lead to friction within teams [63].

For teamwork skills to be equitably assessed, teams need to produce tangible evidence of teamwork. Team charters, planning documents, team meeting notes, and other project management documentation are examples of tangible evidence of the group working as a team. Recording and providing evidence of the contribution of each team member, including the deadlines set and met, helps equitable individual assessment within teamwork.

Widely used peer evaluation of team members [47] needs to be approached with caution. Peer evaluation should not be used as a raw grade modifier as students are not qualified to make objective judgements on the skills of their peers [26]. Hence, Wanner and Palmer [60] recommend using peer evaluation only as a formative feedback tool.

Project grades are a strong predictor of student satisfaction with teamwork [44], with dissatisfaction with grades being mostly accounted for by unhappiness with workload distribution [11]. Much (negative) student feedback focuses on the perception that their grades have been impacted by team mates' social loafing. Thus, designing assessments that increase student engagement while reducing the opportunity for social loafing could increase overall student satisfaction with teamwork.

Designing assessment criteria and marking schemes that allow for marks to be moderated based on contribution can reduce the impetus for social loafing. Furthermore, having one part of a project assessed individually, while another part is assessed as a team, is an approach highly rated by students [63].

3.4 Mentoring and Supervisory Activities

Since the aim of education is to help students learn, it is essential to provide opportunities for students to consult with teaching staff and obtain feedback on progress across the timeline of a project. This consultation could take the form of class time assigned to project work or formal interim submissions [44, 63].

Using scheduled class times for students to work on their projects has the advantage of providing informal and immediate guidance. Finding suitable meeting times outside of class presents a significant challenge for students [63]. Providing some regular scheduled class time should help alleviate this common complaint. Regular and more personal student-staff interactions during project mentoring classes have been shown to lead to positive relationships for staff and students [61]. The increase in asynchronous and remote learning since the start of the pandemic has increased the need to support different ways of enabling staff/student interaction.

Interim submissions are more formal touch points. They may be purely formative, or formally assessed. It is important that expectations are set early on, via the project guidelines, regarding the depth and timelines for feedback on interim submissions. While interim submissions are useful for student teams, care should be taken to not overload teaching teams with interim report marking. Furthermore, students need to be given just the right amount of feedback—enough to steer the project in the right direction, while also allowing independent creative problem solving.

4 Good Practices: Supporting the Development of Teamwork Skills

Designing a team project to support team skills while at the same time covering the requisite curriculum is not an easy task. In this section we detail the literature on the best practices for designing a team project from conception through to completion.

4.1 Designing a Team Project

There are important considerations to keep in mind when deciding to include teamwork in a course. Often, the intention is good, but there is little alignment between the intention and the delivery [24].

When a decision has been made to include teamwork in a course, it is essential to constructively align the team assessment with the learning outcomes of the course [8]. For this to happen, both the tasks involved as well as the assessment criteria used need to value not only the project output but also the process of generating this output. Students will only value teamwork and the project management skills we seek to develop if there are specific marks associated with these skills. Setting up the assessment rubric with separate criteria for teamwork or project management demonstrates that the teacher values these skills and hence, so should the students.

Thus, the assessment guidelines should include explicitly the mechanism and requirements for the allocation of teamwork marks, and the evidence to be submit-

ted. The assessment criteria should clearly state the parts of the project, and the weighting thereof, which will be assessed individually, such as oral presentation skills. Similarly, the parts that will be assessed for the team as a whole such as the technical project report or resultant artifact, should also be clearly indicated.

4.2 At the Start of a Team Project

At the beginning of a team project, the students should be required to develop and agree on a team charter. The charter can include agreement on:

- standards of behaviour
- task breakdown and allocation
- project milestones
- contingency plans if a team member cannot meet a milestone
- team meeting details
- tools and methods to be used for project management
- tools and techniques for technical tasks
- communication methods

The initial submission by the team could be called ‘project proposal’ or similar, and should include the team charter as well as a brief description of the team’s chosen topic. All team members should be required to agree on and sign off on the team charter before submitting it for review by teaching staff.

When the team charter forms part of the project proposal, the assessment criteria should explicitly outline its value. Thus, the submission of the team charter may be awarded marks, may be a hurdle requirement for access to project resources, or may form part of the evidence for a ‘project management’, or ‘teamwork’ criterion evaluated at the end of the project. Teams should be encouraged to start keeping logs and minutes of meetings held (in class and outside of class), and to constantly update and add to the spreadsheet of allocated tasks with associated deadlines, and whether these deadlines have been met. These logs etc could also form part of project management or teamwork evidence.

4.3 Carrying on: The Middle of a Team Project

At the mid-point of the project, or some other similar time, teams should be given an opportunity to revisit their team charter. This creates an opportunity for the team, and each team member to reflect not only on their behaviour as a team member but also their approach to the project thus far. Conflict highlighted at the mid point (or earlier) of a project is much easier to resolve.

All areas of the team charter can be updated. The reasons for updating the team charter, as well as the updated charter, could then be provided as evidence

of continuous project management. Depending on the length and complexity of the project, the team charter may be updated more than once.

At such interim points, teams could be asked to submit a brief project management report outlining the progress of the team thus far, including the dynamics of the teams, conflicts encountered and solutions found. This allows for proactive team management not just by the team, but also enables the teaching team to suggest possible solutions to unresolved conflicts. Early intervention prevents later dissatisfaction. All evidence created in the management of the project so far should also be submitted: meeting notes, notes from consultations with mentors, task allocation, updated weekly plan etc. The teaching staff should ensure that details of the project management documentation required to be submitted, and the level of detail and polish expected, are included in the project assessment instructions.

The submission of the updated team charter and project management progress documentation could accompany the submission of a progress report, or some other interim artefact produced as part of the project work.

As with the initial submission of the team charter, the submission of an updated team charter may be awarded marks, may be a hurdle requirement, or form evidence for assessment at the conclusion of the project.

4.4 Concluding a Team Project

Often, the only evidence that a project has concluded is the submitted project report or artifact. However, for teamwork to be of value to students and the teacher, more needs to be done.

At the conclusion of the project, the team should reflect on the success of their project both in terms of the technical work undertaken and team dynamics. The team could submit a project management report summarising the working of the team and including difficulties encountered and solutions sought and found. Peer evaluations or individual reflections could form part of this submission.

Since evidence of teamwork forms an important part of working in a team, all evidence created in the management of a project should be appended to the end of a project report, e.g.

- attendance records of team meetings and classes that supported the project,
- records of discussions and decisions,
- records of consultation with teaching staff and industry mentors,
- weekly plans,
- records of tasks allocated and completed, including dates of allocation, deadline and completion,
- records of any events that caused deviations from the plan e.g. illness.,
- records of conflict resolution.

The project management report and evidence can be appended to the project report and submitted with the artefacts of the project. Knowing that the contributions

are being recorded and submitted is more likely to make each team member accountable for their contributions to the project outcomes.

5 Case Studies in Teamwork: RMIT University Master of Cyber Security

Given the socio-technical nature and the importance of teamwork in cybersecurity, teamwork is built in at each level of the RMIT University Master of Cyber Security. It is envisaged that a full-time student will have at least one team-based assessment item in each teaching period to ensure development of teamwork skills across their degree. These teamwork assessments range from small teams in introductory courses (Case Studies in Cyber Security) to larger teams for higher year projects (Information Systems Risk Management). Finally, in the first of the two second year projects, the Industry Awareness Project, students work in teams of 2 or 3, before, often, transitioning to industry placements in the Industry Linkage Project.

5.1 Small Team Project in an Introductory Professional Skills Course

Case Studies in Cybersecurity is a core introductory course in the RMIT Master of Cyber Security. Students work in small teams (2–3 students) to investigate a contemporary cybersecurity challenge, reporting on that challenge at the end of semester, in both written and oral formats to an imagined non-technical business audience. The written discussion paper is worth 40% of the course grade, and the oral presentation is worth 20% of the course grade. Individual assessments make up the remaining 40%.

In this introductory course, students are allowed to choose their own teams and their own topic, which seems to work fairly well. At the beginning of the teaching period, students are required to submit a project proposal, which includes a team charter, weekly plan, and topic proposal. There are sample team charters available via library resources, which most students use as a starting point for their own team charter.

Students are required to maintain a detailed log of their meetings; notes taken, week-by-week plans, tasks allocated, and tasks completed. This forms part of the ‘work practices’ criterion which forms the assessment of the teamwork.

At the mid-point of the teaching period, students submit an outline of the discussion paper along with an updated team charter, updated weekly plan, and project management logs. The mid-point submission provides an opportunity for formative feedback on both the discussion paper as well as the team dynamics.

At the end of the teaching period, all project management documents are appended to the written discussion paper and submitted. The work practices criterion is worth 25% of the discussion paper grade (that is, 10% of the overall course grade). If no project management documentation is submitted then the team receives a score of 0 for work practices, a significant grade penalty.

The evidence provided by submitting the team charter and project management logs can be used in the case of a student appealing their grade, or for a plagiarism hearing.

In some years students have delivered team oral presentations, while in other years oral presentations have been delivered individually. Having individual presentations seems to be more widely liked by students, which correlates well with studies which show that students like a combination of individual and team assessment.

5.2 Medium Size Teams in a Final Year Business Skills Course

Information Systems Risk Management is a core business skills course in the RMIT Master of Cyber Security. Students work in larger teams (4–6 students) to conduct a risk management case study, aligned with the international Risk Management Standard (ISO AS/NZS 31000), for a contemporary organisation, making this a simulated Work Integrated Learning (WIL) course.

The risk management case study project starts with choice of the company, asking for justification of choice. This is the first hurdle for the teams—to think of organisations as something more than their cybersecurity profile. The Standard speaks of the need for “communication and consultation”.

The project requires students to gather open source data about their chosen company as they have no access to proprietary company data. Not only do students need to decide which information is relevant, but also, at the same time, make decisions about the reliability of the data gathered, since the quality of the information gathered dictates the effectiveness of the risk management conducted. Given that risk management is the assessment of the unknown, teams face the added difficulty of deciding what information is missing.

The perceived technical nature of cybersecurity, and the mostly technical background of the students, rises to the fore in this course. The most important part of managing risks for any organisation is the context in which it operates. However many of the teams struggle to go beyond well-publicised cybersecurity threats, finding it very hard to think more broadly and deeply about the context of their case study organisation. Using class time to mentor teams becomes essential in this case: the teacher’s task becomes one of convincing students that risk management involves more than the risk assessment of known threats.

With the larger teams, project management also becomes more of an issue: larger teams are often more culturally diverse and take longer to make decisions. In addition, social loafing becomes harder to detect. Project management, thus, is

an essential part of managing team expectations and performance, and is worth 20% of each project submission; in total 9% of the course grade.

The risk management case study has six assessment submissions: project proposal, two interim reports, final report, oral presentation, and peer review. The final report is worth 20% of the course grade with the other submissions worth between 2.5% and 7.5%. The entire risk management case study contributes 60% to the course grade. Breaking the large case study task into multiple smaller submissions encourages students to have a go as they perceive the smaller submissions as ‘do-able’ [9].

Teaching staff mark the project proposal and interim reports at least 1 week before the next item is due. Feedback is provided to the teams on their strategy both for the risk management exercise as well as project management. Timely feedback ensures that errors of judgement can be fixed before too much work had been done. The final report consists of the three interim reports (with corrections) and the final part of the risk management case study.

Oral presentations are delivered after the risk management case study report has been submitted. This parallels the common industry practice of presenting findings to senior managers. Students present as a team, but are graded individually, with assessment criteria for presentation skills, knowledge, and answering questions.

All in all, students acknowledge that this course taxes them the most. However, upon completion of an internship (in their final semester in the degree, via the course Industry Linkage Project), most Master of Cyber Security students report that, out of all of their courses, the skills they learnt in the Information Systems Risk Management course were the most useful to them in their internship.

5.3 Teams in Technical Elective Courses

Technical courses are just as suited to team projects as the professional and business skills courses. In a cybersecurity student’s future career, technical work will be conducted in teams. Hence, there are team assessments in a variety of technical elective courses within RMIT’s Master of Cyber Security.

Industry readiness requires students to be able to apply technical skills in a variety of situations [13]. Introductory technical courses require mastery of concrete technical skills, which can be learnt collaboratively, but are better assessed individually. If team based assessment is used on concrete skills, it’s possible a student may be able to hide their lack of technical skills. However, applied technical projects simulating industry scenarios are suitable for learning teamwork skills.

Technical projects often have artefacts that can make for natural interim submissions. Artefacts such as a problem description, a risk analysis, a wireframe design, a budget, a prototype, or some data analysis could form part of an interim submission. Submission of planning documents and project management logs at these interim submission points supports student teams in developing good project management

habits and allows teaching staff to intervene in any challenging team dynamics or technical misunderstandings.

Allowing students to work on their technical projects during class time, allows the teaching team to assist with skill application and technical solutions. Often no specialist equipment is required for a cybersecurity project, unlike engineering or science projects. Generous site licences and virtual machines allow, in most cases, the necessary software to be installed on a student's own laptop. Using class time allows for active mentoring to support teams to apply concepts and build solutions.

5.4 Small Teams in Capstone Projects

Capstone projects draw together the many skills a student has acquired across their degree. These may include technical skills in hardware and software, analysis and problem solving skills, the use of a variety of data analysis techniques, business skills in strategy and risk management, communications skills tailored to a variety of audiences, and project skills including teamwork.

In the Industry Awareness Project, students work in small teams (2 or 3) to investigate a contemporary industry challenge. There are multiple submissions across the teaching period including team registration, project proposal, progress report, draft report, final report, oral presentation, and peer review. A team charter and project management logs are submitted with each of the interim report submissions.

Providing feedback to peers and juniors is part and parcel of a career in industry. Peer review provides an opportunity to build this skill, allowing students to examine the skills of their peers and evaluate them against the assessment criteria. Students are expected to write in a professional manner as though advising their peers on areas for improvement. The peer review is not used to modify the grades of team members in the project report.

During the Industry Awareness Project, students contact cybersecurity professionals to get advice and perspectives on their topic. Evidence of attempts at industry contact are marked as part of the progress reports. Students can then use their industry contacts to request an industry mentor for the Industry Linkage Project. Teaching staff also work with the RMIT's industry engagement teams and other business units (e.g., RMIT Cyber Ready Cloud Innovation Centre, RMIT IT Services) to negotiate industry projects and internships.

The Industry Linkage Project is the capstone course for the Master of Cyber Security. In this project, students have a cybersecurity professional as an industry mentor. Students can either work in small teams on a project proposed and guided by the industry mentor, or the industry mentors can host students via an internship in their organisation. Multi-disciplinary teams with students from other degrees are possible based on the interest of the industry mentor, and the degree structure. Having an industry partner propose the topic, or act as a client for the project deepens the relevance of the project and can lead to employment opportunities [22].

The final assessment task is a written reflection on their learning journey in teamwork, project management, and working with industry mentors. Basing the final assessment task on non-technical aspects emphasises to cybersecurity students the importance of teamwork, project management, and collaboration skills to their future career. Working well with an industry mentor, or in an internship, requires every good project management and teamwork skill developed in earlier courses.

6 Discussion

Including teamwork in university courses requires attention to be paid to a variety of aspects. The use of team charters, project management logs, constructively aligned assessment criteria, and team mentoring can all create a positive environment that enables students to develop teamwork skills alongside their discipline specific cybersecurity skills.

6.1 Supporting Project Management Skills

Some cybersecurity roles are project based, such as consultancy work, while other cybersecurity roles consist more of a continuous flow of tasks, such as in the security operations centre. The common part of each of these roles is the requirement for cybersecurity professionals to work in teams.

Selecting highly capable and conscientious team members is an obvious advantage in any team task [7]. However, in reality, diverse cohorts in both educational and workplace settings results in having to work with people across a range of conscientiousness.

A good team charter can support teams who may otherwise struggle to work together [18]. Setting up the team charter at the beginning can be considered an intervention that reduces the amount of time spent in resolving conflicts. This is time and energy better spent by students on the technical output of their projects.

Detailed planning and record keeping are at the heart of good project management practices [30]. There are formal project management methodologies for managing large projects, however these are not in the core curriculum for a cybersecurity degree. Understanding the value of formally managing projects develops an aptitude for project management skills.

Providing time in class for students to work on their projects is highly correlated with student satisfaction [44]. Regular class time allocated to the team assessment project supports active engagement of students with their teamwork project across the teaching period, leading to greater project success, and greater team satisfaction.

6.2 Supporting Reflective Learning

There are many ways of supporting reflective learning in a team setting.

A team charter constructed at the beginning of the project encourages students to introspect about their own strengths, weaknesses, goals, work habits, and motivations [40]. Updating the team charter for an interim submission encourages students to reflect on their continuing learning journey both individually and as a team.

Evaluating project success and learning from the process requires detailed records that can be examined [30]. Detailed project management logs and planning documents provide students with the data they need to meaningfully reflect on the process of working as a team. This reflection allows teams to come up with ways of encouraging more participation from teammates and the teaching team to provide feedback on the methods proposed.

Peer evaluation creates very good formative feedback opportunities and supports reflective learning. Peer evaluation can allow a student to vent frustration about their team members, which could explain the strong correlations with project satisfaction and the use of peer evaluation [44]. Peer evaluations are best used as a reflective learning and formative feedback tool [60], rather than a way to assign grades to the team members being evaluated.

Clearly, assigning marks for the submission of a quality team charter or detailed project management logs provides students with extrinsic motivation to engage with the teamwork aspect of team assessments. For some students, such extrinsic motivation can lead to a transactional approach and only superficial learning of teamwork skills [11].

Interim submissions provide useful prompts for reflective learning. Written or formative feedback from the teaching team at interim points of the project provides students with a formal opportunity to reflect on both their project output as well as how their team is working to achieve the output.

Using class time for students to work on their project allows for informal discussions with teaching staff across the project time-span [63]. Providing teaching staff with a set of discussion prompts that encourage reflection on team dynamics can increase teams' engagement in reflective learning.

6.3 Supporting the Creation of Evidence for Grading

Evaluating individual contributions to a team task can be difficult. A good team project results in a highly integrated output, not a collection of individual contributions. The documentation provided in the team charter, project management write-up, and project logs assists in understanding the quality and quantity of students' contributions to a larger project; thus supporting equitable grading [39]. It

also enables teams to submit a request for differential marking and for teaching staff to be able to justify the same.

The students set up the team charter and allocate tasks themselves. The contribution to each sub-task is recorded by the students, so each student's contribution is tracked and logged across the project. There is transparency in the way marks are allocated, leading to more satisfied students [39].

In some projects, students are given the opportunity to evaluate each of their team members [29]. While peer evaluation can be useful in informing the teaching staff when awarding grades, student evaluations should be used with caution. Students are not objective discipline experts; their evaluation of each other's work is not reliable, and may be biased towards friendships [26].

Constructively aligning some of the assessment criteria with the quality of team charters and project logs ensures that students are motivated to put some effort into planning and tracking team member contributions [47]. Allocating marks for the process of working in a team could incentivise a transactional approach to team interactions [11]. However the reduction in opportunities for un-penalised social loafing outweighs any detriment caused by extrinsic motivation.

A good team charter, project logs, and well-written assessment criteria can thus provide evidence for differentiated grading amongst team members on a team assessment item.

6.4 Supporting Student Engagement and Satisfaction

A team charter is both a written and a psychological contract. The team charter includes mutually accepted expectations about the contributions and behaviours of the each team member [29]. Having made an agreement with the team, a student is also making a commitment to engage with the course.

Social Exchange Theory [17] states that people are most satisfied with their relationships when the exchange is balanced. A team charter provides a framework for students to set up expectations such that all team members have a balanced exchange of their resources, time, skills, and prior IP. Equitable exchanges of resources creates trust in relationships. Project logs, including minutes of team meetings, allow for tracking that this exchange remains equitable.

Equitable and transparent allocation of workload within a team project is highly correlated with student satisfaction [11]. Having a team charter provides such a framework for equitable and transparent workload breakdown. Detailed project logs maintain accountability for workload allocation across the project timeline, and provide evidence of and means for addressing, any inequitable behaviour.

6.5 *Supporting Creative Problem Solving*

Our cybersecurity adversaries are highly diverse, requiring us to be creative in defending against their attacks [45]. Working together with people with different life experiences broadens the perspectives on possible solutions. A team charter provides a framework for developing constructive ways of working with people with different experiences, knowledge, skills, and motivations. Diverse teams can find more creative solutions to tricky problems [48].

Assigning class time to work of team assessments allows teams to interact with each other and the teaching staff. Some sharing of ideas amongst the student cohort can lead to creative solutions not previously considered by teaching staff. Peer tutoring across teams can occur organically, uplifting the skills and knowledge of all.

Cybersecurity is a fast moving industry: teaching staff can update their knowledge by discussing contemporary challenges and potential solutions with student teams. The hyper-connectivity now available allows students to find alternative ideas which both challenge and advise their teachers and peers.

7 **Conclusions and Recommendations**

Teamwork is an essential skill in a cybersecurity career. Enabling students to undertake team projects is important for building their teamwork skills, but just providing multiple opportunities for teamwork does not necessarily build the requisite skills. Teamwork is often looked upon by students as an unnecessary evil, leading to poor course feedback. In this paper we discussed ways of improving students' engagement with their teams, thus improving teamwork skills and course satisfaction in these student cohorts.

Finally, we summarise some advice based on our own teaching experiences and the education literature.

- Design multiple opportunities for students to develop their teamwork skills across a course of study. Team learning activities and team assessment tasks contribute to workforce ready graduates.
- Use team assessment tasks only when teamwork is a course learning outcome.
- Explicitly state teamwork and project management skills within the assessment criteria for team assessments.
- Use team charters to support team cohesion.
- Make project management logs part of the assess-able project submission to provide evidence of team members' contribution.
- Allocate class time to team assessment tasks; teaching staff can use this class time to mentor teams in both their technical project output as well as team dynamics.
- Require interim submissions of project work as well as project management summary and documentation. This is an opportunity for formative feedback.

- Use interim submissions and mentoring activities to monitor for social loafing.
- Clearly state how grades are allocated, and the evidence used to allocate grades.
- Have an individually assessed component within a larger team assessment project.

Team assessments can be some of the most memorable experiences in a course of study. With careful design, and active support, it is possible to ensure that cybersecurity students enjoy their team assessments and learn teamwork skills that support their success as they enter the cybersecurity workforce.

References

1. Joshua R. Aaron, William C. McDowell, and Andrew O. Herdman. The effects of a team charter on student team behaviors. *Journal of Education for Business*, 89(2):90–97, 2014.
2. Tristan K. Amador, Roberta A. Mancuso, Erik L. Moore, Steven P. Fulton, and Daniel M. Likarish. Enhancing cyber defense preparation through interdisciplinary collaboration, training, and incident response. *Journal of the Colloquium for Information Security Education*, 8(1):6, 2020.
3. Information Systems Audit and Control Association. ISACA Certifications, undated.
4. Engineers Australia. Accreditation of Engineering Education Programs, undated. Available online. Last accessed September 2022.
5. R. Bancino and C. Zevalkink. Soft skills: The new curriculum for hard-core technical professionals. *Techniques: Connecting Education and Careers (J1)*, 82(5):20–22, 2007.
6. Rufus L Barfield. Students' perceptions of and satisfaction with group grades and the group experience in the college classroom. *Assessment & Evaluation in Higher Education*, 28(4):355–370, 2003.
7. Suzanne T. Bell. Deep-level composition variables as predictors of team performance: a meta-analysis. *Journal of Applied Psychology*, 92(3):595, 2007.
8. John Biggs. Constructive alignment in university teaching. *HERDSA Review of Higher Education*, pages 5–22, 2014.
9. John Biggs and Catherine Tang. *Teaching for quality learning at universities*. Open University Press, Buckingham, 4th edition, 2011.
10. Jane Burdett. Degrees of separation – balancing intervention and independence in group work assignments. *The Australian Educational Researcher*, 34(1):55–71, 2007.
11. Jane Burdett and Brianne Hastie. Predicting satisfaction with group work assignments. *Journal of University Teaching & Learning Practice*, 6(1):70–81, 2009.
12. Cameron Wm. Casper. Teaching beyond the topic: Teaching teamwork skills in higher education. *Journal of Higher Education Theory and Practice*, 17(6):53–63, 2017.
13. Steven T. Cerri. *The fully integrated engineer: Combining technical ability and leadership prowess*. John Wiley & Sons, 2016.
14. Yunjeong Chang and Peggy Brickman. When group work doesn't work: Insights from students. *CBE—Life Sciences*, page ar52, 2018.
15. K. Clark. Myth of the genius solitary scientist is dangerous. *The Conversation*, 17 November, 2017. Available online. Last accessed September 2022.
16. M. Clarke. Rethinking graduate employability: the role of capital, individual attributes and context. *Studies in Higher Education*, 43(11), 2017.
17. Karen S. Cook, Coye Cheshire, Eric R.W. Rice, and Sandra Nakagawa. Social exchange theory. In *Handbook of social psychology*, pages 61–88. Springer, 2013.
18. Stephen H. Courtright, Brian W. McCormick, Sal Mistry, and Jiexin Wang. Quality charters or quality members? A control theory perspective on team charters and team performance. *Journal of Applied Psychology*, 102(10):1462, 2017.

19. J. Dawson and R. Thomson. The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in Psychology*, 9:744, 2018.
20. E. De Prada, M. Mareque, and M. Pino-Juste. Teamwork skills in higher education: Is university training contributing to their mastery? *Psicol. Refl. Crít.*, 35(5), 2022.
21. Carol S. Dweck. *Mindset: The new psychology of success*. Random House Digital, Inc., 2008.
22. Daniel Edwards, Kate Perkins, Jacob Pearce, and Jennifer Hong. Work integrated learning in STEM in Australian universities. *Canberra: Office of Chief Scientist & Australian Council for Educational Research*, 2015.
23. Catherine Gabelica, Sven De Maeyer, and Michaéla C. Schippers. Taking a free ride: How team learning affects social loafing. *Journal of Educational Psychology*, 114(4):716, 2022.
24. Joanne L. Hall and Asha Rao. Non-technical skills needed by cyber security graduates. In *2020 IEEE Global Engineering Education Conference (EDUCON)*, pages 354–358. IEEE, 2020.
25. Julie M. Haney and Wayne G. Lutters. Cybersecurity advocates; discovering the characteristics of an emergent role. *Information and Computer Security*, 29(3):485–499, 2021.
26. Stephanie J. Hanrahan and Geoff Isaacs. Assessing self-and peer-assessment: The students' views. *Higher Education Research & Development*, 20(1):53–70, 2001.
27. Mariana Hentea and Harpal S. Dhillon. Towards changes in information security education. *Journal of Information Technology Education*, 2006.
28. Veronica Conway Hughston. *Consequences of team charter quality: Teamwork mental model similarity and team viability in engineering design student teams*. PhD thesis, The Pennsylvania State University, 2014.
29. Phillip Hunsaker, Cynthia Pavett, and Johanna Hunsaker. Increasing student-learning team effectiveness with team charters. *Journal of Education for Business*, 86(3):127–139, 2011.
30. Project Management Institute. *A guide to the project management body of knowledge (PMBOK guide)*. Project Management Institute, Newtown Square, Pennsylvania, 6th edition. edition, 2017.
31. International Information System Security Certification Consortium. CISSP – the world's premier cybersecurity certification, undated.
32. International Information System Security Certification Consortium. ISC² certifications, undated.
33. International Information Systems Security Certification Consortium. *(ISC)² Workforce Study 2020*. International Information System Security Certification Consortium, 2020.
34. William H.A. Johnson, David Baker, Longzhu Dong, Vas Taras, and Charles Wankel. Do team charters help team-based projects? The effects of team charters on performance and satisfaction in global virtual teams. *Academy of Management Learning & Education*, 21(2):236–260, 2022.
35. Prashant Khanna, Diab Abuaiadah, and Chris Baker. Forming team for cybersecurity and cyber-forensics operations using individual profiling. In *Proceedings of the 12th Annual Conference of Computing and Information Technology Education and Research in New Zealand*, pages 49–65, 2021.
36. Soo Ling Lim and Peter J. Bentley. Diversity improves teamwork: optimising teams using a genetic algorithm. In *2019 IEEE Congress on Evolutionary Computation (CEC)*, pages 2848–2855. IEEE, 2019.
37. David Livingstone and Kenneth Lynch. Reflections on 'group project work and student-centred learning'. *Journal of Geography in Higher Education*, 26(2):213–215, 2002.
38. J.D. Looney. Diversity, equity, & inclusion: Why does it matter to leadership development? *The Journal of Character & Leadership Development*, 8(2):60–67, 2021.
39. Nirmal K Mandal. Individual student assessment in team projects: a team charter approach. In *Australasian Association for Engineering Education Annual Conference, AAEE2018 Conference, The University of Waikato, Hamilton, New Zealand*, pages 9–12, 2018.
40. J. E. Mathieu and T. L. Rapp. Laying the foundation for successful team performance trajectories: The roles of team charters and performance strategies. *Journal of Applied Psychology*, 94(1):90–103, 2009.
41. Hajo Meijer, Rink Hoekstra, Jasperina Brouwer, and Jan-Willem Strijbos. Unfolding collaborative learning assessment literacy: a reflection on current assessment methods in higher education. *Assessment & Evaluation in Higher Education*, 45(8):1222–1240, 2020.

42. Australian Nursing and Midwifery Federation. Nursing and Midwifery Registration and Accreditation. Accessed 13 April 2022.
43. A. Peslak and S. Hunsinger. What is cyber security and what cyber security skills are employers seeking? *Issues in Information Systems*, 20(2):62–72, 2019.
44. Elizabeth Pfaff and Patricia Huddleston. Does it matter if I hate teamwork? What impacts student attitudes toward teamwork. *Journal of Marketing Education*, 25(1):37–45, 2003.
45. Winifred R Poster. Cybersecurity needs women. *Nature Comment*, 555:577–580, 2018.
46. Prashanth Rajivan, Michael Champion, Nancy J. Cooke, Shree Jariwala, Genevieve Dube, and Verica Buchanan. Effects of teamwork versus group work on signal detection in cyber defense teams. In *International Conference on Augmented Cognition*, pages 172–180. Springer, 2013.
47. Linda Riebe, Antonia Girardi, and Craig Whitsed. Teaching teamwork in Australian university business disciplines: Evidence from a systematic literature review. *Issues in Educational Research*, 27(1):134–150, 2017.
48. D. Rock and H. Grant. Why diverse teams are smarter. *Harvard Business Review*, 4(4):2–5, 2016.
49. B. Schneider. The importance of security engineering. *IEEE Security & Privacy*, 10(5):88–88, 2012.
50. Carey Singer. Student perception of social loafing in university teamwork. Master’s thesis, Faculty of Commerce, Organisational Psychology, University of Cape Town, 2019.
51. Peter Stewart. Four vital considerations for your team charter. Forbes, August 2022. Available online. Last accessed September 2022.
52. Cathy Stone, Jill Downing, and Janet Dyment. *Improving Student Retention and Success Within the Context of Complex Lives and Diverse Circumstances*, pages 161–178. Springer International Publishing, Cham, 2021.
53. Chiara Succi and Magali Canovi. Soft skills to enhance graduate employability: comparing students and employers’ perceptions. *Studies in Higher Education*, 45(9):1843–1847, 2019.
54. Therese E. Sverdrup and Vidar Schei. Cut me some slack: The psychological contracts as a foundation for understanding team charters. *The Journal of Applied Behavioral Science*, 51(4):451–478, 2015.
55. Therese E. Sverdrup, Vidar Schei, and Øystein A. Tjølsen. Expecting the unexpected: Using team charters to handle disruptions and facilitate team performance. *Group Dynamics: Theory, Research, and Practice*, 21(1):53, 2017.
56. N. Thompson. *People skills*. Bloomsbury Publishing, 2021.
57. Karen L. Tonso. The impact of cultural norms on women. *Journal of Engineering Education*, 85(3):217–225, 1996.
58. Joni Tornwall, Elizabeth A. Fitzgerald, and David Hrabec. Team charters in group work. *Journal of Nursing Education*, 60(5):302–302, 2021.
59. B. von Solms and R. von Solms. Cybersecurity and information security – what goes where? *Information and Computer Security*, 26(1):2–9, 2018.
60. Thomas Wanner and Edward Palmer. Formative self- and peer assessment for improved student learning: the crucial factors of design, teacher participation and feedback. *Assessment & Evaluation in Higher Education*, 43(7):1032–1047, 2018.
61. Paul Wellington, Ian Thomas, Irene Powell, and Brian Clarke. Authentic assessment applied to engineering and business undergraduate consulting teams. *International Journal of Engineering Education*, 18(2):168–179, 2002.
62. Jessica L. Wildman, Daniel M. Nguyen, Ngoc S. Duong, and Catherine Warren. Student teamwork during COVID-19: Challenges, changes, and consequences. *Small Group Research*, 52(2):119–134, 2021.
63. Laura Wilson, Susie Ho, and Rowan H. Brookes. Student perceptions of teamwork within assessment tasks in undergraduate science degrees. *Assessment & Evaluation in Higher Education*, 43(5):786–799, 2018.

Towards a Light-Weight Certification Scheme for Cybersecurity MOOCs



Matthias Beckerle, Argyro Chatzopoulou, and Simone Fischer-Hübner

1 Introduction

While the number of cybersecurity breaches and crimes are steadily growing, there is at the same time an increasing lack of cybersecurity experts meeting the demand for cybersecurity skills in Europe and world-wide [1]. A recent survey on this so-called cybersecurity skills gap [2] showed a direct relation between the lack of cybersecurity experts and security breaches occurring in organisations, leading to the loss of revenue, recovery costs, and/or fines. Cybersecurity education has to enable professionals to commit to lifelong learning due to the rapidly evolving nature of cybersecurity [3].

In the recent years and especially during the COVID-19 pandemic, the demand for MOOCs (Massive Open Online Courses) has considerably grown [4]. MOOCs are increasingly used as part of academic education and as a means for promoting lifelong learning. They can play an increasingly important role as an educational tool for addressing the cybersecurity skills gap.

However, for learners and for organisations interested in cybersecurity MOOCs as a means for competence development of their employees, it is not always easy to evaluate the quality of cybersecurity MOOCs that are offered. Especially for practical online cybersecurity training that has recently emerged, involving virtual cybersecurity tools or cyber ranges, the quality of such cybersecurity education may depend on many factors. This includes not only the cybersecurity qualification of the

M. Beckerle (✉) · S. Fischer-Hübner
Department of Mathematics and Computer Science, Karlstad University, Karlstad, Sweden
e-mail: matthias.beckerle@kau.se; simone.fischer-huebner@kau.se

A. Chatzopoulou
TÜV TRUST IT GmbH, TÜV Austria Group, Vienna, Austria
e-mail: argyro.chatzopoulou@tuv.at

proposer or instructor but also technical features of the cyber range, ethical routines for handling incidences that are followed and taught, etc.

Existing quality assurance frameworks for MOOCs (see e.g. [5–7], and the work presented in a recent literature review [8]) have a general scope and have not defined quality criteria specifically for cybersecurity MOOCs. Moreover, to the best of our knowledge, no certification scheme for (cybersecurity) MOOCs have been proposed yet, which only requires reasonable efforts and costs and is thus suitable to be used in practice for the “quality branding” of cybersecurity MOOCs. The research objective of our work conducted within the scope of the EU H2020 projects CyberSec4Europe¹ and CONCORDIA² and reported in this article is to develop building blocks for a quality evaluation framework and practical “lightweight” certification scheme for the quality branding of cybersecurity MOOCs in Europe and beyond. The EU Cybersecurity Act has introduced a EU-wide cybersecurity certification framework, which could also in future be complemented with a certification scheme for the quality branding of cybersecurity MOOCs.

To this end, we extended existing quality assurance frameworks for MOOCs by eliciting quality criteria for cybersecurity MOOCs to be offered in Europe including academic MOOCs, MOOCs for lifelong learning and cyber range MOOCs, which are summarised in Sect. 2). Based on the elicited quality criteria, we propose a quality branding process for cybersecurity MOOCs, presented in Sect. 3), which was validated through trial evaluations. A survey that we conducted with cybersecurity MOOC stakeholders, particularly educators and consumers mostly from Europe, on the suitability of our quality criteria for quality certification is summarised in Sect. 4. It confirmed a high acceptance of the proposed quality criteria but also showed the need for a “light-weight” certification scheme for cybersecurity MOOCs, meaning that the implementation of such a scheme should require limited efforts and costs (for all involved parties). Therefore, we conducted interviews with European certification experts to investigate which quality criteria and with what priority could or should be part of a light-weight evaluation and certification scheme, and how light-weight, effective and flexible certification procedures could be designed. The results of these certification expert interviews are summarised and discussed in Sect. 5 followed by overall conclusions in Sect. 6.

2 Quality Criteria for MOOCs

In the EU project CyberSec4Europe, we have derived and proposed a list of quality assurance criteria for MOOCs, which include both generic and cybersecurity specific quality criteria, which can both be used as a basis for evaluating and branding the quality of cybersecurity MOOCs in Europe. They define criteria that

¹ <https://cybersec4europe.eu/>.

² <https://www.concordia-h2020.eu/>.

should apply for the following types of MOOCs (or for a selection of them): Academic MOOCs issuing credit points for enrolled university students, continuous (life-long) learning MOOCs and future cyber range MOOCs. The criteria were derived from (1) conclusions from a review of existing European MOOCs in terms of gaps to be addressed, (2) regulations and ethical standards and are also based on (3) criteria taken from existing quality assurance frameworks for MOOCs (including [5–7]) and (4) existing best practices and our experiences (see [9]). The list below provides the main categories of the quality criteria and summarises their main requirements (for more details, please refer to [10] and confer with [9]).

QC1—Qualification of the Proposer The proposing institution (proposer) should have the proper qualification and experience to be able to develop, run and evaluate the MOOC in a professional manner, and be recognised by relevant cybersecurity stakeholders. The proposer of an academic MOOC should be a recognised higher education institution and have expertise in applied technology & private-public partnership. For cyber range MOOCs, the proposer’s cyber range should be technical, work-life oriented which can mimic realistic phenomena (attack campaigns, threat actors, techniques & tools) from the cyber security field.

QC2—Qualification of Participants The MOOC should be as inclusive as possible for enhancing cyber security competence in Europe. Participants must also be able to find out whether they are qualified for a MOOC and/or why they are not accepted for enrolment. For this reason, it is important that the acceptance process should be legit and transparent. The participants must have the qualifications needed for taking the MOOC. For cyber range MOOCs, the participants should have the skills to operate a technical cyber range platform, unless this is taught in the course.

QC3—Qualification of Instructors The qualification of the instructors (teachers) is fundamental to ensure a high quality of a MOOC. The instructors (teachers) must have an academic degree and/or teaching experience and should have a pedagogical education. For a cyber range MOOC, one of the instructors should have technical skills for conducting and supervising operations.

QC4—Examination and Credentialisation For awarding credits or certificates, a course examination that is conducted has to verify that learning goals have been achieved in a transparent manner. Therefore, any cyber range activities, laboratory work, and assignment that are mandatory for obtaining a course credential should be clearly specified. Course certificates should always be issued for recognition of the educational achievements in the professional or life-long/blended learning context. Academic European MOOCs should be recognised as a valid credit-awarding course within the European credit transfer system.

QC5—Course Evaluation Means for continuous and anonymous (online) course evaluations by participants should be in place.

QC6—Meeting Professional Expectations Suitable (cybersecurity) stakeholders, especially from working life and the employment side, should be involved throughout the MOOC development and operation. When providing a cyber range course

to a company or an organisation, it should be “realistic enough”, i.e. simulate operational and supporting services and systems available for the participants.

QC7—Course Structure, Content and Evaluation The MOOC should provide an overview presenting its goals and structure, the main content, format, reference literature, language, knowledge and skills as prerequisites, as well as the learning outcome to be acquired. The MOOC should cater for different learning styles and strategies to reach the learning outcomes. Proposers should review the MOOC and its content periodically, so that the content reflects state of the art and continues to fulfil its learning goals.

Continuous learning MOOCs offered by companies should not with an inappropriate bias promote commercial products or systems of that company, unless the entire focus of the MOOC is on the teaching or training of the usage of these products or systems.

QC8—Course Platform and Channels Only platforms and channels that comply with the EU General Data Protection Regulation (GDPR) must be selected. Moreover, the functionality of the platform should comply with the EU Directive 2016/2102 on the accessibility of the websites and mobile applications of public sector bodies for ensuring accessibility and inclusiveness.

QC9—Openness Openness should be guaranteed both in terms of the MOOC content and material (by using an open licensing, e.g. CC-BY-SA, allowing to freely reuse, mix and redistribute material), as in terms of being open and adapting to the learner’s needs, enabling them to study at any time, place and pace of choice. There should be clear, transparent and justifiable policies for defining any restrictions to digital openness (e.g. for the use of malicious or attack code for teaching purposes) and/or openness of course elements (e.g. those that are hacking-related or for other reason security-sensitive) to learners for ethical or security reasons.

QC10—Ethics Cybersecurity MOOCs should due to the sensitivity of the subject (methods of attacks, exploitation of vulnerabilities, implementation of measures) introduce and enforce ethical principles for cyber security courses in regard to ethical hacking, handling and reporting security-sensitive information and processing of personal data.

QC11—Privacy The MOOC owner that has the GDPR role of a data controller must ensure that all personal data of course participants and instructors are processed in compliance with the GDPR and other applicable laws. Especially, the platform and course instances storing personal data must be secured by appropriate security controls and should follow the privacy by design and by default principle (Art. 25 GDPR) and provide a transparent privacy policy. While privacy criteria must in general be considered for all types of MOOCs, they are especially relevant to cybersecurity MOOCs teaching security and privacy, for demonstrating that privacy and security controls taught in the course are also enforced in practice, i.e. the course should live up to the standards taught.

QC12—Utilising Cyber Ranges The institution’s cyber range should provide systems and services for planning, running and doing post-exercise analysis and for allowing the defending team to prevent, detect, mitigate and recover from cyber incidents.

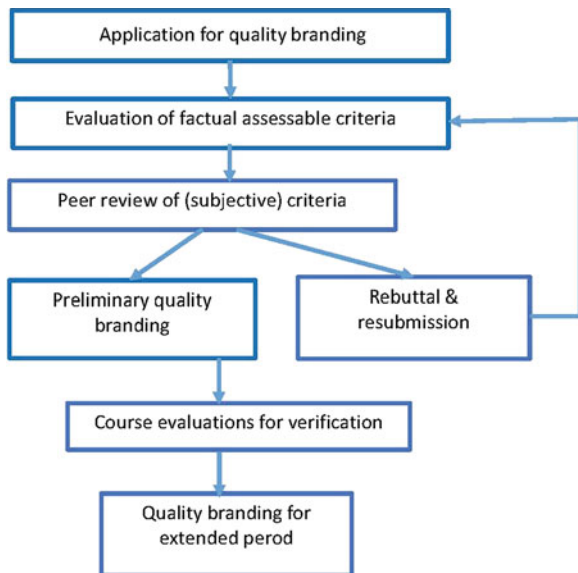
It should be pointed out that the criteria listed above related to EU data protection and accessibility regulation are specific for Europe, even though they may be easily adapted or extended to laws in regulations in other countries outside the EU for making the quality criteria assurance catalog below also applicable for the quality branding of MOOCs to be used in non-EU countries.

3 Evaluation Process

In this section, we describe the initial proposal for a quality branding process for MOOCs, which we derived for the CyberSec4Europe project and which was validated with an internal exemplary evaluation that we conducted earlier for a selection of academic and lifelong learning cybersecurity MOOCs offered by European providers [9, 10]. The proposed process consists of the following eight steps that are also shown in Fig. 1:

1. **Application:** In the first step, the institution seeking a quality branding submits its application including documentation demonstrating how quality criteria have been met by them, when they submit their application for a quality branding.

Fig. 1 Steps of the quality branding process suggested in [10]



2. **Evaluation of factual assess-able criteria:** In step 2, all criteria that can be objectively assessed are evaluated. These are criteria that are measurable by a third party, and/or are fulfilled if an official legal document or internal policy document that is required exist. For instance QC1 requiring that the proposer of an academic MOOC should be a recognised higher education institution is an example for a factual assess-able criteria.
3. **Peer-review of criteria:** In step 3, all remaining quality criteria that are subjective are evaluated by a group of at least 3 experts in a peer-review process. In this peer-review process, the experts first assess the fulfilment of the criteria independently based on their expertise and experiences. Then a discussion of all reviews takes place among the experts followed by a moderated consensus meeting for agreeing on an assessment and decision. If all criteria are fulfilled, step 6 follows next. For instance, QC7 requiring no inappropriate bias for commercial MOOCs, or QC9 requiring that policies for defining any restrictions to digital openness should be clear, transparent and justifiable are examples of criteria that require a peer-review.
4. **Rebuttal and resubmission phase:** Only MOOCs that clearly fulfil all quality criteria that are not formulated as optional should be quality branded. For any non-optional criteria that are not met, partly met or not clearly met, the proposer should be requested to address these open issues first and then resubmit the application for a quality branding.
5. **Repeat step 2–4:** Upon re-submission, steps 2–4 are repeated.
6. **Preliminary Quality branding for first-time MOOCs:** Ultimately, active participation in a MOOC might be needed to reliably retrieve all information needed for the evaluation. Even creating an account and subscribing to a course often does not provide all information needed, since some MOOCs are not active at the moment of review and the related information is not (yet) retrievable. If a MOOC runs for the first time, a preliminary assessment and quality branding should be given that is re-evaluated after the first iteration of the MOOC is completed.
7. **MOOC evaluation by course participants for verification:** Any preliminary quality branding evaluation is complemented by gathering feedback from students that participated in the MOOC. If the course evaluations reveal issues in regard to the practical fulfilment of the quality criteria, these issues need to be addressed and re-evaluated through step 2–4 before the period for the quality branding can be extended.
8. **Quality branding for an extended time period:** If all quality criteria are met for a MOOC that has been successfully given at least once, a quality branding can be awarded for a longer time period. It is important to decide how often a provided quality branding should be re-evaluated since MOOCs naturally are subject to changes and may get outdated. While ideally, a revaluation should happen after each iteration of a MOOC for considering any changes, the costs and time for re-evaluations need to be considered as well. Hence, longer periods for 1–3 years for the validity of quality brands may be appropriate.

4 Certification Criteria for Cyber Security MOOCS

In this section, we present the results of a survey that we conducted to investigate if our findings align with the opinions of stakeholders from academia and industry, particularly those that earlier took roles as cybersecurity MOOC consumers or educators. This section presents parts of the results published in [11] where additional details can be found. The survey was conducted within the scope of the EU Horizon 2020 projects CONCORDIA and CyberSec4Europe for addressing the following research questions:

- **RQ1:** How do cybersecurity MOOC stakeholders value a certificate as a selection criteria and what should such a certificate convey?
- **RQ2:** What challenges have current cybersecurity MOOC stakeholders experienced?
- **RQ3:** What quality criteria do stakeholders want to be included in a certification scheme for addressing such challenges?

This section is based on [11] where additional information can be found.

4.1 Methodology

To answer our three research questions an online survey was conducted. We utilized the tool EUSurvey,³ (a tool supported by the European Commission's ISA² programme, promoting interoperability solutions for public administrations, businesses and citizens) to design, publish and collect the responses.

This user study was approved by one of the Ethical Advisors at Karlstad University and started in January 2021. We sent the survey questions to various cybersecurity mailing lists (including mailing lists operated by FOSAD, IFIP TC11, and the Swedish and German cybersecurity mailing lists SWITS and FBSEC) framed as a survey on Cybersecurity MOOC Certification.

4.2 Study Design

We asked in total 72 questions in the survey:

- 8 questions in the demographic part to collect demographic information,
- 11 quantitative questions in part A about former experiences with MOOCs,
- 5 Likert scale questions in part B about criteria that factor in the selection of a specific MOOC

³ <https://ec.europa.eu/eusurvey/>.

- 6 Likert scale questions in part C about which statements or properties should be conveyed by a MOOC Certificate,
- 20 quantitative questions in part D1 about challenges encountered by the participants during their MOOC experience (5 of those questions are specific for Cybersecurity MOOCs and only appear when such a participation was confirmed),
- 20 Likert scale questions in part D2 about quality aspects that should be included in a (Cybersecurity) MOOC Certification,
- an open questions regarding what other challenges could be addressed by a relevant certification scheme,
- and optionally the participants email address (for being contacted for further feedback).

The questions can be seen in the Tables 1, 2, 3, 4, and 5.

4.3 Demographics

We received answers from people living in 15 different countries, with the majority coming from Spain, Greece, Sweden, and Germany. Most participants were between 25 and 65 years old. 50% were educators, 62% of the participants identify as male and 33% as female, what is in the computer science context a relatively large percentage of female participants.⁴

4.4 Results

We received valid answers from 86 participants. Fifty-six of those participated in at least one MOOC and 27 participated in cybersecurity related MOOCs. In total our participants participated in 282 MOOCs. For Part A and Part D1 the amount or percentage of relevant MOOCs are reported. Since 50% of our participants were educators, we decided to investigate if there is a difference between educators and non-educators. The results can be seen in the Tables 1, 2, 3, 4, 5, and Fig. 2.

4.5 Discussion

The instructor and quality rankings by other users were agreed by most MOOC stakeholders as a factor that plays an important role in the selection of a MOOC.

⁴ <https://isc2-center.my.salesforce.com/sfc/p/#G0000000iVSt/a/0f000000bpXo/sQxPX9KxnuiioZxNWxDGLJIitkyOFsg9GOPdRo4h44TM>.

Table 1 Questions and results, part A: “In how many of the MOOCs have you had the following experiences?” [11]

Part	μ (%)	Experience
A1	25	Real time instructions
A2	78	Prerecorded instructions
A3	88	Course curriculum in digital format
A4	35	Real time Q&A
A5	79	Non real time Q&A
A6	12	No interaction
A7	63	Communication with other participants
A8	28	No communication with other participants
A9	23	Cyber MOOC: practical aspects
A10	51	Cyber MOOC: material regarding practical aspects
A11	35	Cyber MOOC: no practical aspects

Table 2 Questions, part B: “Which of the following criteria should factor in the selection of a MOOC?” [11]

Part	Agree (%)	Dis-agree (%)	Criteria
B1	59	15	The brand name of the MOOC provider.
B2	81	2	The instructor.
B3	69	8	The credential that is provided after a participant has concluded the training (e.g. attendance affirmation, completion certificate, badge etc).
B4	72	6	A certificate saying that the MOOC was reviewed and fulfils specific acknowledged criteria.
B5	81	6	The quality ranking of the MOOC by other users (e.g. user ranking, comments etc).

Table 3 Questions, part C: “If a certification scheme for MOOCs existed, what should the respective certificate convey?” [11].

Part	Agree (%)	Dis-agree (%)	Aspect
C1	84	5	The quality of the instruction material follows specific acknowledged international best practices.
C2	56	14	The platform used for the provision of the MOOC follows relevant acknowledged international best practices.
C3	84	5	The instructor used for the provision of the MOOC meets specific prerequisites in terms of competence (technical and educational).
C4	56	13	The availability of the platform is monitored, measured, analysed and evaluated.
C5	74	7	The entire MOOC experience (as a sum and the individual components) is regularly reviewed and optimised.
C6	67	7	The MOOC platform and experience has been designed based on international accessibility best practices for supporting social inclusion of users with disabilities or special learning needs.

Table 4 Questions and results, part D1: “When using a MOOC platform, identify whether any of the below were challenges that you faced.” [11]

Part	μ (%)	Challenge
D1.1	36	<i>1. Qualification of the proposer</i>
		The proposer was neither a recognised academic institution nor another type of institution that has built a reputation with certified courses.
D1.2	18	<i>2. Qualification of instructors</i>
		The MOOC was not taught, examined or supervised by a person with the necessary educational and technical skills.
D1.3	23	<i>3. Course examination, credentialisation and recognition</i>
		The assessment methods did not align with the learning objectives or were not measured by valid means.
D1.4	21	The skills, knowledge or abilities covered through the MOOC and the respective examination had not been defined.
D1.5	21	<i>4. Meeting professional expectation</i>
		The MOOC content did not reflect the state of the art.
D1.6	16	<i>5. Course structure and content criteria</i>
		The MOOC did not have all the components that were needed to follow and understand the course content by the participants.
D1.7	17	The material was of poor quality or outdated.
D1.8	41	The MOOC did not allow for different learning styles and strategies to reach the leaning outcomes.
D1.9	11	The assignments, examples and case studies were not aligned with the learning outcomes.
D1.10	15	The MOOC did not have specific learning outcomes defined for the course.
D1.11	39	<i>6. Openness</i>
		The MOOC did not enforce openness to learners by adapting to their needs.
D1.12	40	The platform, material and experience did not comply with accessibility regulations.
D1.13	19	<i>7. Security & privacy of the platform</i>
		The teaching platform was not secure.
D1.14	38	The teaching platform did not comply with privacy principles as stated in the GDPR.
D1.15	48	The teaching platform was operated by a non-European provider and it was not clear whether personal data were transferred to a country outside of Europe in compliance with GDPR rules.
D1.16	27	<i>8. Cybersecurity courses and exercises</i>
		The cybersecurity exercises were not technical or work-life oriented.
D1.17	30	Cybersecurity experts/stakeholders were (not) involved in the course development.
D1.18	31	Hacker ethical rules were not taught during the course.
D1.19	13	Rules for restricting for course participation were not fair or transparent.
D1.20	31	The exercise environment was not realistic or not aligned with the course learning objectives.

Table 5 Questions and results, part D2: “Which of the following quality aspects should be certified by a certification scheme for cybersecurity MOOCs for addressing these challenges?” [11]

Part	Agree (%)	Dis-agree (%)	Quality aspect
D2.1	73	15	The type of the organisation proposing the MOOC.
D2.2	87	7	The competency of the people involved in the delivery of the MOOC and the related examination.
D2.3	80	5	The criteria for the design and implementation of the assessment.
D2.4	49	13	The self-assessment ability.
D2.5	85	8	The information contained in the MOOC.
D2.6	69	12	The completeness of the MOOC.
D2.7	86	6	The quality of the material.
D2.8	51	13	The flexibility of the MOOC for effective performance.
D2.9	79	6	The course content in relation to the learning outcomes.
D2.10	87	3	The learning outcomes.
D2.11	50	12	The adaptability of the MOOC.
D2.12	67	8	The accessibility performance.
D2.13	75	10	The security of the MOOC platform.
D2.14	87	6	The privacy friendliness and GDPR compliance of the platform.
D2.15	83	7	GDPR compliance for third country data transfers.
D2.16	82	8	The practical examples of cybersecurity training.
D2.17	67	8	The involvement of relevant interested parties.
D2.18	76	4	Hacker ethical rules.
D2.19	80	4	Fairness and transparency.
D2.20	78	4	Quality of the cyber range infrastructure.

A large majority (72%) also sees a MOOC certificate as a selection factor. Also the fact that 81% of our participants are considering the quality rankings by other users shows us that there is a need for information about the quality of MOOCs. User ratings can however be quite easily manipulated, which could be another argument for rather having an official certification process in place.

Non-educators agreed even slightly more often than educators that the instructor should be factored in when selecting MOOCs. Hence, we could not observe any obvious bias by educators overestimating their importance. These results also indicate that quality criteria for the qualification of the instructor will play an important role in a certification scheme, although the exact way how this could be factored in remains still an open issue.

Only 26 out of 56 MOOC stakeholders answered the two openness related questions D1.11 and D1.12, whereas all other questions about general experiences with MOOCs were answered by at least 53 participants. One possible explanation could be that those stakeholders who skipped the questions were not sure if it was a problem of their MOOCs, as they may not need accessibility features themselves

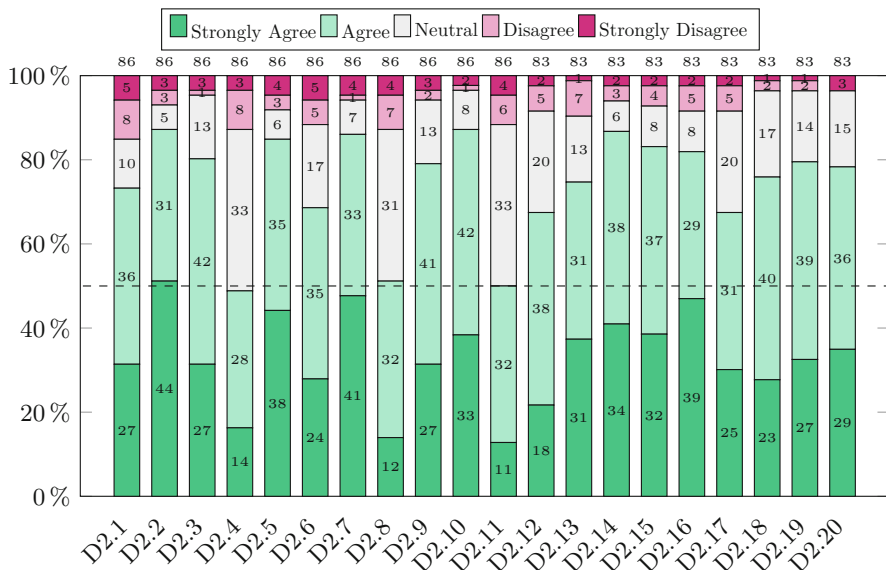


Fig. 2 Answers to the questions of part D [11]

and therefore did not pay attention to those feature and thus did not perceive accessibility as a challenge directly. Therefore, the result that 43% of those who answered the relevant questions had encountered accessibility issues should be interpreted with caution.

The result that *privacy of MOOC platforms* was perceived as a major challenge does not come as a surprise given that most of the leading MOOC platforms are hosted by non-EU providers. This means that data about the MOOC participants including sensitive information about their course performance and activities may flow to a third country outside the EU without adequate data protection in non-compliance with the GDPR and its chapter V.

Therefore, privacy including GDPR compliance can be seen as an important criteria, also from the stakeholders’ perspectives, for the quality branding by a European cybersecurity MOOC certification scheme.

The survey results also help answering our research questions as described below:

4.5.1 RQ1: How Do Cybersecurity MOOC Stakeholders Value a Certificate as a Selection Criteria and What Should Such a Certificate Convey?

Answers to Part B of the survey showed that a majority of the MOOC stakeholders (both educators and non-educators) value a MOOC certificate showing that a

MOOC was independently reviewed and fulfils specific acknowledged criteria, and agreed using it as a factor for selecting a MOOC. Moreover, the majority of survey participants chooses that all suggested quality aspects in Part C should be conveyed by a certification scheme.

4.5.2 RQ2: What Challenges Have Current Cybersecurity MOOC Stakeholders Experienced?

Answers to Part D1 of the questionnaire reveal that all challenges in the questionnaire were also experienced by at least some of the MOOC stakeholders. Most of the experienced challenges that were reported are related to privacy, accessibility, and openness. However, issues concerning the instructors' qualification, the quality of the proposer, undefined learning goals, or learning goals not aligned with the examination were also experienced by many stakeholders.

4.5.3 RQ3: What Quality Criteria Do Stakeholders Want to Be Included in a Certification Scheme for Addressing Such Challenges?

Our survey participants largely agreed that the quality criteria in Part D2 should be included in a certification scheme to address the highlighted challenges. The respondents (educators and non-educators) generally agreed that the proposed criteria should be included in a certification scheme for cybersecurity MOOCs, while also providing information on their prioritisation (e.g. D2.7: the quality of material vs. D2.4: the self-assessment ability). A further analysis is needed to weight the relevant criteria against the best practices and decide on the final set. Finally, the actual criteria and the structure of the certification scheme should be derived by also taking into consideration the points mentioned in Sect. 4.5, the concerns raised by the open questions and the results of the further analysis.

5 Interviews with Certification Stakeholders

In this section, we present the results of structured interviews that we conducted within the scope of the EU Horizon 2020 projects CONCORDIA and Cyber-Sec4Europe to identify the criteria for a Certification Scheme for Cybersecurity MOOCs. As mentioned in Sect. 4, a majority of the MOOC stakeholders (both educators and non-educators) value a MOOC certificate showing that a MOOC was independently reviewed and fulfils specific acknowledged criteria, and agreed on the value of using it as a factor for selecting a MOOC. It was however also pointed out, that such a MOOC certification scheme could only be successfully deployed if the time, efforts and costs for certifications and re-certifications were limited. In other words, it was noted that the certification scheme should be "lightweight" and

flexible while at the same time effective and well suitable to achieve its objectives. The number, type and complexity of quality criteria as well as the work that needs to be conducted for a certification of MOOCs and re-certification of any MOOC updates are all factors that need to be considered for designing a light-weight MOOC certification scheme.

In order to evaluate and form a proposal for a “light-weight” Cybersecurity MOOC Certification Scheme and its quality certification criteria, it was decided to conduct structured interviews with European stakeholders from the Certification Ecosystem (Certification Bodies, National Cybersecurity Authorities, Accreditation Councils). The interviews allowed us to collect both qualitative data on the reasons for their answers as well as quantitative data on their preferences and rankings of criteria. The selected stakeholders and their organizations represent main actors involved in the design, development, implementation and accreditation of cybersecurity certification schemes, and thus are in the best position to provide input on requirements for a light-weight certification scheme and preferences for specific criteria that could be incorporated in such a certification scheme.

5.1 Demographics

In total, 12 interviews were conducted. Eleven of the interviewees represented Certification Bodies and 1 represented a National Cybersecurity Authority. The participants represented organizations from the following countries: Austria, Cyprus, France, Greece, Italy, Serbia, Spain and Sweden. Almost all certification bodies that were represented conduct international business, meaning they perform audits and certification in more than one country. 42% (5 out of 12) of the interviewees were female and 58% (7 out of 12) of the interviewees were male. Finally, the participants had a collective experience in the certification industry of more than 120 years with most of them having more than 10 years of experience.

5.2 The Content of the Interviews

The objectives of the interviews were to investigate (1) what quality criteria could or should be with what priority part of a (light-weight) cybersecurity MOOC evaluation scheme, and (2) how a light-weight and flexible certification procedure can be designed.

The interviews were conducted during April 2022 by one of the authors and were split into three parts:

Part 1 (split between the beginning and the end), provided introductory information on Cybersecurity MOOCs (short definition of what MOOCs are, which are the specific characteristics of Cybersecurity MOOCs), described the objectives of

the interviews, asked general anonymous demographic information, notified on the terms of processing and requested the relevant consent.

Part 2 introduced the various quality criteria and the results of their evaluation through our previous survey (as reported in Sect. 4). Specifically, the opinion of the interviewees was solicited on the following:

- **If and how the instructor and quality rankings by other users could be incorporated in a Cybersecurity MOOC Certification Scheme.** Both criteria were agreed by most survey participants as important criteria for selecting a MOOC (see Table 2). Our interest was to discuss with the experts how far these criteria could be suitable evaluation criteria for a light-weight scheme.
- **If and how a regular review and optimization of the MOOC experience could be added in a Cybersecurity MOOC Certification Scheme.** Answers to this question can help us with designing a light-weight scheme that flexibly allows the re-certification of revised MOOCs with low efforts and costs.
- **The desirability of and preference for the quality criteria identified in the interviews** (to be incorporated in Cybersecurity MOOC Certification Scheme). The ranking of evaluation criteria can help us to prioritise criteria that should go into a certification scheme in case we would like to restrict the number of criteria, in an effort to make it more affordable.
- **The complexity of incorporating the quality criteria identified in the interviews in a Cybersecurity MOOC Certification Scheme.** Answers to these questions are directly important for making a certification scheme light-weight in terms of the complexity of conducting a certification.

The data collection of this part of the interview was supported by a survey implemented in the EUSurvey tool,⁵ due to the number of criteria discussed (20 distinct criteria to be ranked based on their desirability and complexity). The link to the tool and the relevant password was provided to the participants during the interview and they were allowed to fill it in during or after the interview.

Part 3 was an open discussion on the subject of a cybersecurity MOOC certification scheme. For this part of the interview, notes were taken and later evaluated.

5.3 *The Results of the Interviews*

5.3.1 **Comments on the Selection of criteria (Points 5.2.1. and 5.2.2.)**

83.33% of the Interviewees (10 out of 12) agreed that the instructor could be added in a cybersecurity MOOC certification scheme. When asked how the instructor could be incorporated within the scheme, all answers concentrated on the

⁵ <https://ec.europa.eu/eusurvey/home/welcome>.

competency of the instructor and how this could be evaluated within the certification scheme and subsequent audit. The evaluation methods suggested were: Interview sessions with the instructors during the audit, review of relevant documents of experience and knowledge and implementation of a specialized skills certification scheme for the instructor.

83.33% of the Interviewees (10 at of 12) agreed that verified users' reviews could be added in a cybersecurity MOOC certification scheme. When asked how this could be incorporated within the scheme, all answers suggested that each cybersecurity MOOC participant should have the ability to easily provide an evaluation in a common and easy to understand representation, and the result of this evaluation should be visible to all interested parties. It was also pointed out that such a mechanism could be manipulated, and to protect the value of the mechanism additional measures were recommended such as: creation of an independent third party registry of reviews, incorporation of the duration of use of the platform and random verification of the reviews.

58.33% of the Interviewees (7 at of 12) agreed that regular review and optimization of the MOOC experience could be part of a cybersecurity MOOC certification scheme. 25.00% of the Interviewees (3 at of 12) disagreed whereas 16.67% (2 out of 12) did not provide an opinion. When asked how this could be incorporated within the scheme (for the positive responses), the interviewees stressed that a regular review mechanism should be incorporated to make sure that the information, mechanism, content, material and platform remain valid and updated. On the other hand, the rest of the respondents argued that the reviews of the participants could provide a more continuous review mechanism.

5.3.2 Comments on the Desirability of the Criteria (Point 5.2.3.)

The interviewees were requested to rank 20 quality criteria based on their desirability. A criterion was defined as desirable by a participant, if the participant perceive that the incorporation of this criterion within a cybersecurity MOOCs certification scheme would be of increased value (to the evaluation process, the evaluation results and to the stakeholders).

The results are depicted in Fig. 3 (series Name: Question 4—represented in the figure by green squares). The axis Average Ranking represents the position the participants have awarded to the respective criterion in terms (in this series) of desirability. The lowest the value, the highest position, the more desirable the criterion. The results can thus be divided into three categories: Most desired, medium desired, less desired.

Most Desired

- (C1) The quality of the material
- (C2) The learning outcomes
- (C3) The competency of the people involved in the delivery of the MOOC and the related examination
- (C4) The course content in relation to the learning outcomes

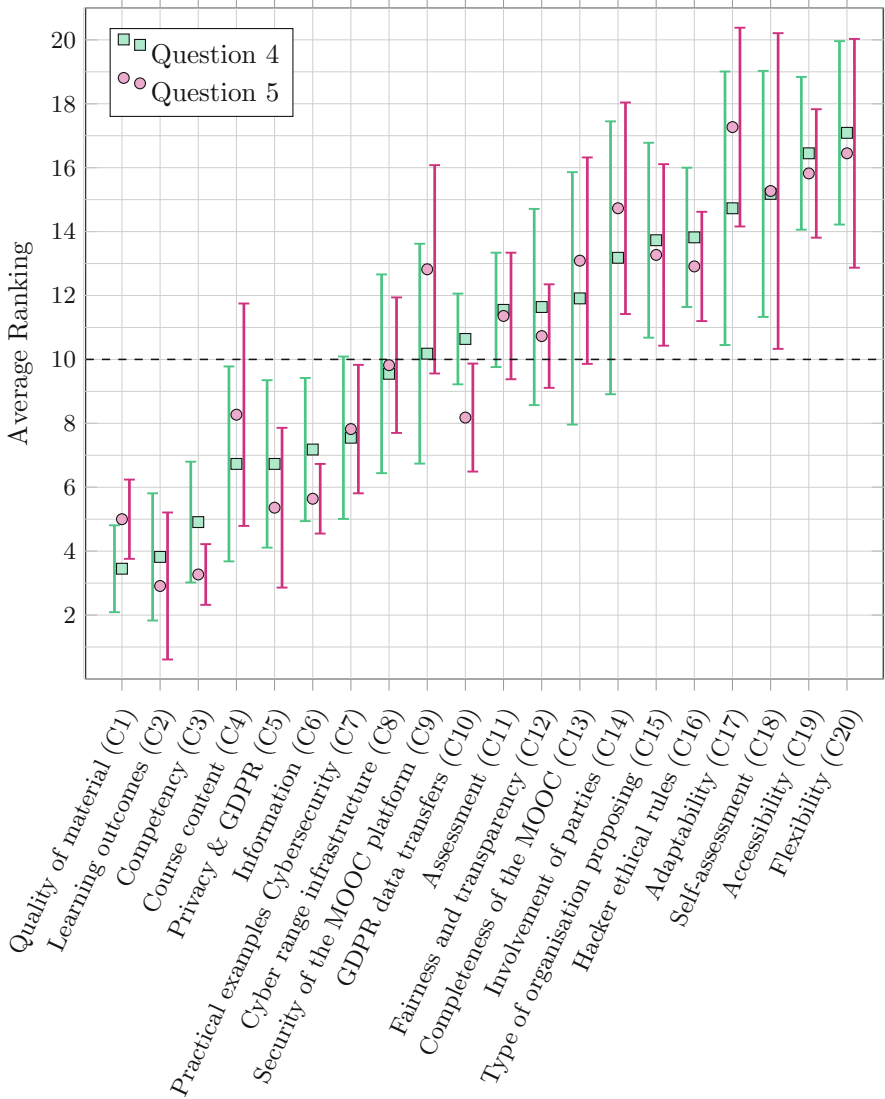


Fig. 3 Average ranking of each criterion as rated by the experts including related confidence intervals with confidence level 95%; sorted by Question 4 from most desirable (left) to least desirable (right); lower means more desirable (Question 4) or easier to implement (Question 5)

- (C5) The privacy friendliness and GDPR compliance of the platform
- (C6) The information contained in the MOOC
- (C7) The practical examples of Cybersecurity training

Medium Desired

- (C8) Quality of the cyber range infrastructure
- (C9) The security of the MOOC platform
- (C10) GDPR compliance for third country data transfers
- (C11) The criteria for the design and implementation of the assessment
- (C12) Fairness and transparency
- (C13) The completeness of the MOOC

Less Desired

- (C14) The involvement of relevant interested parties
- (C15) The type of the organisation proposing the MOOC
- (C16) Hacker ethical rules
- (C17) The adaptability of the MOOC
- (C18) The self-assessment ability
- (C19) The accessibility performance
- (C20) The flexibility of the MOOC for effective performance

The quality of material, the learning outcome and the competency of the persons involved in the delivery of the MOOC and the related examination appear to be characteristics identified as most desirable by the majority of the participants.

These criteria are closely followed by the privacy friendliness and GDPR compliance of the platform, the course content in relation to the learning outcomes, the information contained in the MOOC and the practical examples of Cybersecurity training.

The self-assessment ability, the accessibility performance and the flexibility of the MOOC for effective performance score lowest in terms of desirability based on the interviewees responses.

5.3.3 Comments on the Complexity of the Criteria

The interviewees were requested to rank the criteria mentioned above based on their complexity. The complexity was to be judged in relation to the implementation of each criterion within a cybersecurity MOOC certification scheme. A criterion can be desirable but at the same time may be too complex to be implemented within a scheme. This would lead to a “heavy” and rigid certification scheme, which in turn would hinder the adoption and use of the certification scheme. The results are depicted in Fig. 3 (series Name: Question 5—represented in the figure by pink circles). The axis “Average Ranking**” represents the position the participants have awarded to the respective criterion in terms of complexity. The lower the value, the higher the position, the easier is the implementation of the criterion.

The learning outcomes, the competency of the people involved in the delivery of the MOOC and the related examination and the quality of the material appear to be characteristics identified as easy to implement by the majority of the participants.

These criteria are closely followed by the privacy friendliness and GDPR compliance of the platform, the information contained in the MOOC, the GDPR compliance for third country data transfers and the practical examples of Cybersecurity training.

The self-assessment ability, the accessibility performance, the flexibility of the MOOC for effective performance and the adaptability of the MOOC have been identified as the most complex in terms of implementation within a Cybersecurity MOOC Certification Scheme.

5.3.4 Differences of Opinion

The majority of the answers vary between the different respondents. In this section, some examples and comments are provided on these differences of opinion for both desirability and complexity.

More than half of the respondents ranked the adaptability of the MOOC at the last quarter of the desirability scale (positions 19 and 20 out of 20) and the rest placed it in the second quarter (positions 5, 7 and 8). Almost all of the respondents rated its implementation at the highest levels of complexity. The reasoning behind this difference of uniformity and compatibility between the desirability and complexity, may lie in the definition of adaptability. Specifically and in relation to the MOOC performance, as stated above, adaptability is defined “as being open and adapting to the learner’s needs, enabling them to study at any time, place and pace of choice”. This is a generic and very open definition, without any existing standard or framework to easily quantify or evaluate it. For this criterion to be incorporated in a possible certification scheme, it would need to be further refined and detailed.

Another example is the security of the MOOC platform. In this case also more than half of the respondents ranked it at the first half of the desirability scale (positions from 2 to 7 out of 20) and the rest placed it in the second half (positions 13–17). However, more than half of the respondents ranked it at the first half of the complexity scale (meaning of increased complexity). The respondents further commented that security of an online platform is a technical issue that has increased complexity and an increased scope. To this, they added that there are several standards containing requirements for security in applications (e.g. OWASP Application Security Verification Standard (ASVS),⁶ Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities.⁷ In these case, the competences of the persons performing these audits would be technical (from a security point of view), which greatly differs from the competences needed by the auditors of other criteria proposed. Finally,

⁶ <https://owasp.org/www-project-application-security-verification-standard/>, SP 800-218.

⁷ <https://csrc.nist.gov/publications/detail/sp/800-218/final> etc. Each of these standards has a different objective and specific audits (on process or product) need to designed and implemented to evaluate them.

it was proposed that since this is a desirable characteristic of a MOOC platform, the requirement should be incorporated, implemented and regularly controlled by the organization (e.g. run independent penetration test from reputable sources), and during the audit, the auditor should only review the relevant documentation (e.g. penetration test reports, issues raised and their subsequent treatment) rather than conducting a technical audit.

5.3.5 Agreements

While the majority of the answers vary between the different respondents, there are also some cases of convergence of opinion. In this section, some examples and comments are provided on agreements that were shared for both desirability and complexity. For example, in the case of the accessibility performance of the MOOC, the majority of the respondents placed it on the lowest positions regarding both desirability and easiness of implementation (high complexity). The comments of the respondents on this subject revolved around the fact that accessibility is a complex subject, covering many categories and standards, which by themselves should be subject to individual audits. Moreover, it was stressed that accessibility is not just about providing the ability to change font size or color contrast. A MOOC platform and course should be designed and produced in such a way as to maximise their foreseeable use by persons with disabilities, as also stated for other types of products in the European Accessibility Act of 2019.

Another example is the case of the competences of the people involved in the delivery of the MOOC and the related examination. In this case, the respondents ranked it in relatively high position regarding both desirability and easiness of implementation (low complexity). As discussed above, there are various solutions for incorporating this criteria into a cybersecurity MOOC certification scheme. In terms of complexity (and keeping in mind that the need for the resulting scheme to be as lightweight as possible), the competence of the people involved in the delivery of the MOOC and the related examination, could be accomplished through the review of relevant documentation as evidence of competence and the review of parts of the course delivery.

5.4 Discussion

It was generally acknowledged by the interviewees that a cybersecurity MOOC certification scheme would be useful, especially since the COVID-19 pandemic crisis has increased the importance and usage of cybersecurity MOOCs. Although all of proposed criteria could, in principle, be incorporated within a certification scheme, one of the success factors would be to make it light and flexible enough to achieve a greater adoption by the market—especially since following such a certification scheme would be voluntary. So, when selecting criteria to be incorporated

within a cybersecurity MOOC certification scheme, desirability should be weighed against the complexity of implementation. Finally, it should be pointed out that when drafting the certification scheme, the audit technique used also contributes to complexity (e.g. as mentioned before for the security criterion). Hence, for a criterion that is highly desirable but complex, an investigation should be carried out to identify the technique that could achieve the desired result without noticeably increasing the audit complexity (e.g. review of documentation of tests instead of performing the tests).

6 Conclusions

Finally, in order to define building blocks for a “lightweight” certification scheme for future quality branding of cybersecurity MOOCs, we propose a priority-order of evaluation criteria for a quality labeling process as outlined in Sect. 3.

Our goal was to generate a ranking of the quality criteria that combines how desirable they are and how easily they can be implemented as part of a certification scheme. By combining the results from our survey with MOOC stakeholders (see Sect. 4) with the results from the interviews with certification experts (see Sect. 5), the following ranking of criteria can be derived (see Table 6).

The following criteria received the best combined rankings from MOOC stakeholders and certification experts, were rated to be easier to be implemented and should be part of a lightweight evaluation scheme:

- The learning outcomes.
- The quality of the material.
- The competency of the people involved in the delivery of the MOOC and the related examination.
- The privacy friendliness and GDPR compliance of the platform.
- The information contained in the MOOC.
- The course content in relation to the learning outcomes.
- The practical examples of Cybersecurity training.
- GDPR compliance for third country data transfers.
- Quality of the cyber range infrastructure.

The following criteria received medium combined rankings from MOOC stakeholders and certification experts and should at least be considered to be part of a lightweight evaluation scheme:

- Fairness and transparency.
- The criteria for the design and implementation of the assessment.
- The security of the MOOC platform.

The following criteria received the lowest combined rankings from MOOC stakeholders and certification experts, were rated to be more difficult to be implemented

Table 6 Combined Order of Criteria; a lower number means that the criterion is more desirable to be part of the certification scheme, and in case of “Complexity” it means that it is simpler and thus less complex to implement according to the certification experts

Criterion	Combined	MOOC stakeholders	Certification experts	Complexity
Learning outcomes (C2)	1	1	2	1
Quality of material (C1)	2	4	1	3
Competency (C3)	3	3	3	2
Privacy & GDPR (C5)	4	2	5	4
Information (C6)	5	5	6	5
Course content (C4)	6	11	4	8
Practical examples cybersecurity (C7)	7	9	7	6
GDPR data transfers (C10)	8	6	10	7
Cyber range infrastructure (C8)	9	10	8	9
Fairness and transparency (C12)	10	7	12	10
Assessment (C11)	11	8	11	11
Security of the MOOC platform (C9)	12	13	9	12
Hacker ethical rules (C16)	13	12	16	13
Involvement of parties (C14)	14	15	14	16
Completeness of the MOOC (C13)	15	17	13	14
Type of organisation proposing (C15)	16	16	15	15
Accessibility (C19)	17	14	19	18
Adaptability (C17)	18	19	17	20
Self-assessment (C18)	19	20	18	17
Flexibility (C20)	20	18	20	19

and should be only be optionally part of an evaluation scheme, e.g. if specifically requested by the MOOC provider:

- Hacker ethical rules.
- The involvement of relevant interested parties.
- The completeness of the MOOC.
- The type of the organisation proposing the MOOC.
- The accessibility performance.
- The adaptability of the MOOC.
- The self-assessment ability.
- The flexibility of the MOOC for effective performance.

It is important to note that even the lowest ranked criteria are still considered desirable by MOOC stakeholders and certification experts. In addition, criteria directly stating legal requirements (such as privacy requirements derived from the GDPR or accessibility requirements pursuant to the EU Accessibility Act) have to be implemented independent of their rankings.

The EU Cybersecurity Act of 2019 establishes a EU-wide cybersecurity certification framework for products, processes, services. While this cybersecurity certification framework is so far not focusing on the certification of educational service or cybersecurity skills, we think that our work can contribute to closing this gap in future by providing important input for defining a certification scheme for the quality branding of cybersecurity MOOCs. This may in turn promote the cybersecurity MOOC market and increase the overall quality of cybersecurity MOOC offerings. Especially, cybersecurity MOOCs with a high and baseline quality branding can help educating competent cybersecurity professionals and thus contribute to higher cybersecurity standards and practices.

References

1. European Cybersecurity Agency ENISA: Higher Education in Europe: Understanding the Cybersecurity Skills Gap in the EU (2021)
2. FORTINET: 2022 Cybersecurity Skills Gap – Global Research Report. <https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf> (2022)
3. John, S.N., Noma-Osaghae, E., Oajide, F., Okokpujie, K.: Cybersecurity education: The skills gap, hurdle! In: *Innovations in Cybersecurity Education*, pp. 361–376. Springer, Berlin (2020)
4. Education Technology: COVID-19 drives considerable growth in demand for MOOCs. <https://edtechnology.co.uk/international/covid-19-drives-considerable-growth-in-demand-for-moocs/> (2021)
5. Commonwealth of Learning: *Guidelines for Quality Assurance and Accreditation of MOOCs*. Commonwealth of Learning (2016)
6. Rosewell, J., Jansen, D.: The OpenupEd quality label: Benchmarks for MOOCs. *The International Journal for Innovation and Quality in Learning* **2**(3), 88–100 (2014)
7. Stracke, C.M., Tan, E., Teixeira, A., Vassiliadis, B., Kameas, A., Sgouropoulou, C., Vidal, G.: Quality Reference Framework (QRF) for the Quality of MOOCs. <http://www.mooc-quality.eu/QRF> (2018)
8. Stracke, C.M., Trisolini, G.: A systematic literature review on the quality of moocs. *Sustainability* **13**(11) (2021). <https://doi.org/10.3390/su13115817>
9. Fischer-Hübner, S., Beckerle, M., Lafuente, A.L., Martínez, A.R., Saharinen, K., Skarmeta, A., Sterlini, P.: Quality criteria for cyber security moocs. In: *IFIP World Conference on Information Security Education*, pp. 46–60 (2020). Springer
10. S. Fischer-Hübner et al.: *CyberSec4Europe Deliverable 6.1 – Case Pilot for WP2 Governance*. <https://cybersec4europe.eu/publications/deliverables/> (2019)
11. Beckerle, M., Chatzopoulou, A., Fischer-Hübner, S.: Towards cybersecurity mooc certification. In: *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pp. 1–11 (2021). IEEE

Learning Environments for Digital Forensics Teaching in Higher Education



Leslie F. Sikos 

1 Introduction to Teaching Digital Forensics in Higher Education

Digital forensics, which not long ago was considered a pseudoscience only, recently became a prominent component of cybersecurity ecosystems, and is now based on industry practices as well as scientific or scientifically backed techniques, procedures, and processes. Some debate whether digital forensics should be considered a distinct academic discipline and whether it is a profession in its own right, and there are four main positions: (1) digital forensics considered as a branch of computer science, (2) digital forensics as a branch of forensic science, (3) digital forensics as an interdisciplinary science, and (4) digital forensics as a distinct discipline [18]. In contrast to, and sometimes in combination with, cybersecurity incident detection, which is typical to *security operation centers (SOCs)*, *security information and event management (SIEM)*, and *security orchestration, automation, and response (SOAR)*, which focuses on the timely detection of cyberattacks in live network traffic, digital forensics has a focus on the retrospective analysis of network traffic captured in datasets (network forensics, cloud forensics, IoT forensics) and/or traces of malicious software or nefarious user activities on computing systems (computer forensics, mobile forensics, database forensics, etc.). However, a large share of the relevant data can be considered sensitive, even personal, often with *personally identifiable information (PII)*. As such, teaching digital forensics poses many challenges in terms of how to generate realistic/authentic datasets that do not expose sensitive data, whether personal or corporate. The latter should be avoided because disclosing technical details of IT infrastructures publicly can make organizations

L. F. Sikos (✉)
Edith Cowan University, Perth, Australia
e-mail: l.sikos@ecu.edu.au

more vulnerable to cyberattacks. For this reason, as a general rule of thumb, organizations do not disclose their corporate data publicly, while mimicking the network traffic or computing devices of large enterprises—which would be required for students to develop hands-on skills that can be used in the industry and is a fundamental need for employability in this field—requires resources that typically go beyond university budgets as well as lecturer’s time and effort disproportional to the duration and workload associated with a single-semester unit. In addition, if only datasets are used for teaching, the initial steps of digital forensic investigations, such as data acquisition in a forensically sound manner, and final steps, such as presenting artifacts to a court of law as an expert witness, are not replicated in class, and therefore these cannot be taught efficiently or at all. There are limited options to overcome this, one of which is using *mock trials*, which, however, require an actual criminal court judge presiding over the proceedings and having an actual jury [25]—definitely not something that could be arranged for each and every class.¹ How technical terms of digital forensics can be explained by expert witnesses to laypersons for trials in a courtroom setting can alternatively be demonstrated using multimedia presentations [6]. Another option is specializing to a subdomain of digital forensics, such as data acquisition from various IoT devices, for example, and provide alternate experimental learning opportunities for this [40].

Beyond technology, the other main educational path for graduate-level education in this field is digital investigation management [21, 22]. Even focusing on the technical aspects of digital forensics comes with its own challenges. While analyzing even a single volume of a storage medium can be effective for teaching file system basics, file signatures, and hashing via active learning and constructivism [23], the forensic investigation of modern-day computing systems requires sophisticated environments, equipment, and tools, while actual *field works* are often not possible to arrange. Just the sheer variety of computing devices ranging from servers, workstations, desktop computers, laptops, tablets, IoT devices, and smartphones to cloud-based hosting and “as a service” and storage solutions itself poses an ever-growing challenge to digital forensic investigators because of data heterogeneity issues, not to mention the data volume generated by these devices and services, nor the unaffordability of industry-leading digital forensic software tools to educational institutions and students.

1.1 From Knowledge and Skills to Competencies

Digital forensics is multidisciplinary by nature, having components of computing, traditional forensic science, law, social sciences, criminal justice, and various other disciplines, which should be considered when developing digital forensics curricula

¹ This is why most digital forensics classes focus predominantly or exclusively on the technical aspects of, and to a lesser extent, publicly disclosed laws related to, digital investigations.

[28, 29]. The practical aspects of the field justify training for, and certification of, skills for applications, tools, procedures, and practice, while teaching digital forensics in higher education can provide knowledge, abstraction, tool development, establishing procedures, and theory [39]. Digital forensics practitioners require competence that can only be achieved through academic education, training, and certification (which will be complemented over time by work experience) [34], and therefore digital forensic investigator training requires competency-based assessment methods [31]. Graduates in digital forensics need to be able to demonstrate, and therefore undergraduate digital forensics degrees should cover, a solid background knowledge and skillset in a range of fields, covering an in-depth understanding of the following areas [2, 8, 24]:

- Computer hardware
- Computer software, in particular, operating systems
- Communication networks
- Programming concepts
- Investigation techniques
- Relevant parts of the (federal) criminal justice system: applicable local, state, national, and international laws
- Relevant parts of sociology and psychology to understand human motivations

Because state-of-the-art digital forensic investigations employ artificial intelligence as well, such as machine learning and automated reasoning [32], teaching the basics of AI to digital forensic investigator trainees and students is also desirable.

Specializing in a subdomain of digital forensics requires a strong background in specific fields, such as IoT authentication in the case of IoT forensics [37], which is not supported by teaching the fundamentals and general concepts, procedures, and practices of digital forensics.

Those seeking a designation of NSA² CAE-CDE³ with a focus area of digital forensics, the following knowledge units (KUs) are required in a degree: basic scripting or introductory programming, IA fundamentals, introduction to cryptography, IT system components, networking concepts, policy legal ethics and compliance, system administration, networking technology and protocols, operating system concepts, data structures, device forensics, digital investigations, forensic accounting, hardware reverse engineering, host forensics, media forensics, network forensics, operating systems' theory, software reverse engineering, and vulnerability analysis [30].

Skills to develop are not limited to technical skills, such as hands-on skills with digital forensic tools, but also to meticulous record-keeping, the ability to write on technical issues to non-technical audiences in layman's terms [2], and the ability to handle, manage, and investigate computer evidence while maintaining the chain of custody [19].

² National Security Agency

³ Centre of Academic Excellence—Cyber Defence Education

Digital forensics was historically available only at pre-tertiary levels such as bootcamps or short courses on specific digital forensics software tools, operating systems, and hacking [4], industry certificates, diplomas/advanced diplomas, and at some universities as individual units rather than entire course offerings [33]. Some examples are *COMP6445 Digital Forensics* of the University of New South Wales, *COMP 5071 Digital Forensics Essentials* of the University of South Australia, or *CSG2305 Computer Forensics* of Edith Cowan University. However, over time, digital forensics became available in the form of Bachelor degree programs, still mainly in the U.S. only—see the *Computer Forensics & Digital Investigations* degree of Champlain College⁴ or the *Bachelor of Science in Digital Forensics* of the University of Albany,⁵ or the digital forensics master’s course of the Polytechnic of Leiria [3], for example.

The distribution of digital forensics courses and units across colleges and universities, and the significant gaps in the materials covered and the relevant emerging technologies, urge finding solutions and developing robust higher educational programs in this field [35]. Accreditation and certification of academic degrees in digital forensics are yet to become mainstream, although some certification programs are already in place (e.g., the *National Certification Programme for Academic Degrees in Cyber Security* in the UK, which has notable specializations including digital forensics [12]).

1.2 Learning Theories and Pedagogical Models

Digital forensics training and teaching are globally still inconsistent and ineffective, and curriculum developers often employ off-the-shelf course materials without an overall educational strategy, although efforts have already been made in this area—see, for example, the *European Antitrust Training in Forensic IT (EAT_FIT)* [1] or the *Digital Forensics Framework for Instruction Design (DFFID)* of the SANS Institute [26], a reputable cybersecurity training company. While digital forensics is very much a hands-on field, online digital forensics courses can go beyond merely online correspondence courses by designing them based on well-founded learning theories around active learning, such as *social constructivism*, *resource-based learning*, *collaborative learning* [14], *problem-based learning* [17], *narrative-based teaching* [20], and the *BSCS 5E instructional model*.⁶ This makes it possible to accommodate various learning needs and different learning preferences of students, covering undergraduate and postgraduate courses, in-class/on-campus, hybrid (blended), online, and accelerated online delivery modes.

⁴ <https://online.champlain.edu/degrees-certificates/bachelors-computer-forensics-digital-investigations>

⁵ <https://www.albany.edu/business/programs/bs-digital-forensics>

⁶ Engage, explore, explain, elaborate, and evaluate

Technology-enhanced learning that goes way beyond (multimedia) contents of units shared on learning management systems (LMSes) can be well-utilized in digital forensics teaching, for example, in the form of multi-platform cloud computing infrastructures and computer-based tools, such as the *D-FET* training environment [7].

2 Laboratory Components and Tools for Teaching Digital Forensics

A number of software tools and appliances, hardware, and simulators can be used in digital forensics teaching, as discussed in the following sections.

2.1 Digital Forensics Software Tools

While some argue that freely available, open source software tools (*Autopsy*,⁷ *FTK Imager*,⁸ *DB Browser for SQLite*,⁹ *ExecutedProgramsList*,¹⁰ *AccessData Registry Viewer*,¹¹ *Xplico*,¹² *Wireshark*,¹³ *ExifTool*,¹⁴ *IrfanView*,¹⁵ *HashCalc*,¹⁶ etc.), or freely available (often time-limited) demo versions of commercial software (e.g., *PassMark OSForensics*,¹⁷ *Aid4Mail Forensic*¹⁸), can be suitable for teaching digital forensics even at a tertiary level [16], not teaching mainstream software tools can result in less-than-optimal graduate outcomes in terms of technical skills, which can ultimately effect employability. However, industry-leading digital forensic investigative tools, such as the *AccessData Forensic Toolkit (FTK)*,¹⁹

⁷ <https://www.autopsy.com>

⁸ <https://accessdata.com/product-download/ftk-imager-version-4-2-0>

⁹ <https://sqlitebrowser.org>

¹⁰ https://www.nirsoft.net/utils/executed_programs_list.html

¹¹ <https://accessdata.com/product-download/registry-viewer-2-0-0>

¹² <https://www.xplico.org>

¹³ <https://www.wireshark.org>

¹⁴ <https://www.sno.phy.queensu.ca/~phil/exiftool/>

¹⁵ <https://www.irfanview.com>

¹⁶ <https://www.slavasoft.com/hashcalc/>

¹⁷ <https://www.osforensics.com>

¹⁸ <https://www.aid4mail.com/email-forensics>

¹⁹ <https://accessdata.com/products-services/forensic-toolkit-ftk>

EnCase Forensic,²⁰ *Magnet AXIOM*,²¹ *Nuix Investigate*,²² *Oxygen Forensics*,²³ and *X-Ways Forensics*,²⁴ are typically not affordable for educational institutions in the long run, while student and/or volume licensing is not available (only subscription-based and sometimes individual perpetual licenses).

2.2 Software Appliances for Digital Forensic Investigations

Many open source digital forensic software tools are available as a preinstalled and preconfigured software appliance or virtual machine. These include, but are not limited to, *SIFT Workstation*,²⁵ *CAINE (Computer Aided INvestigative Environment)*,²⁶ *DEFT (Digital Evidence & Forensics Toolkit)*,²⁷ *HELIX3*,²⁸ the *Paladin Forensic Suite*,²⁹ *Kodachi Linux*,³⁰ *Cyborg Hawk Linux* [36], and *Kali Linux*.³¹ While very useful and can be installed by students on their own computers, they are challenging to be used for teaching in a lab environment, where administrative privileges may not be available for security reasons, while using them in a cloud-based, nested virtualized environment (such as in Hyper-V under Microsoft Azure) requires quite a lot of resources, might make the class template difficult to maintain and clone, and/or difficult to deploy to student VMs, and may have serious performance issues.

2.3 OS Virtualization

Virtualized platform environments are used in digital forensic investigations, for example, to analyze a potentially virus-infected Windows instance under Linux without the risk of getting the host machine infected, and in digital forensics teaching, such as to use the aforementioned SIFT Workstation. Both free (e.g., *Oracle VirtualBox*,³² *VMware Workstation Player*³³) and commercial software tools

²⁰ <https://www.guidancesoftware.com/encase-forensic>

²¹ <https://www.magnetforensics.com/products/magnet-axiom/>

²² <https://www.nuix.com/products/nuixinvestigate>

²³ <https://www.oxygen-forensic.com>

²⁴ <http://www.x-ways.net/forensics/>

²⁵ <https://digital-forensics.sans.org/community/downloads>

²⁶ <https://www.caine-live.net>

²⁷ <https://docs.gns3.com/appliances/deft-linux.html>

²⁸ <http://www.e-fense.com/products.php>

²⁹ <https://sumuri.com/software/paladin/>

³⁰ <https://www.digi77.com/linux-kodachi/>

³¹ <https://www.kali.org>

³² <https://www.virtualbox.org>

³³ <https://www.vmware.com/au/products/workstation-player/workstation-player-evaluation.html>

(e.g., *VMware Workstation Pro*³⁴) are available for local virtualization; cloud-based solutions offer a viable alternative for universities teaching digital forensics, although large case study files can result in performance issues and might need to be pre-ingested in Autopsy in the template to be deployed to student VMs so that the ingestion process will use up expensive virtualization time only once rather than for all the student instances. Deploying VMs with pre-indexed datasets in *Splunk*³⁵ for network forensics education also has the benefit of the daily indexing limit of 500 MB of the free version of the software not being applicable to GBs of datasets in the student instances.

2.4 Virtual Learning Environments and Immersive Virtual Reality (VR) for Digital Forensic Investigation Simulators

There are virtual forensic training software environments that are designed for traditional, rather than digital, forensics—see the *Virtual Crime Scene Simulator (VCSS)*³⁶ of the University College Dublin or the computer-based 360° crime scene simulation tool of the University of Lausanne [27], for example. These combine problem-based learning with experimental learning, thereby allowing students to implement transversal theoretical knowledge and different skills in a practical activity that mimics real-world simulated criminal case situations. While such learning activities can be very effective, they require regular feedback and continuous interactions between students and the teaching staff. In contrast, virtual learning environments for teaching digital forensics provide authentic/realistic scenario simulation via a virtual learning and/or virtual reality environment, which simulates authentic-looking communication network infrastructures, configurations, and data traffic, computer storage, realistic but made-up corporate and personal profiles, and the like.

Some of the main components of virtual digital forensics laboratories include networked examination and storage machines, secure communications, multi-factor authentication, role-based access control, and case management and digital asset management systems [9]. Typical virtual digital forensic teaching laboratory activities include artifact gathering, storage, and reporting. These can use resources shared among fellow students/group members, can be geographically distributed, and if in the cloud, online students can access them in their own schedule and use them in their own pace. The three main types of virtual digital forensic laboratories are (1) general-purpose cloud-based virtualized computing environments, such as Amazon AWS and Microsoft Azure, with preinstalled and preconfigured digital forensic software tools, and pre-ingested datasets, (2) Linux distributions

³⁴ <https://www.vmware.com/au/products/workstation-pro.html>

³⁵ <https://www.splunk.com>

³⁶ <https://youtu.be/bqaFhffRFM0>

specifically designed for cybersecurity applications, such as the aforementioned Kali Linux, which has a set of tools that can be used for digital forensic laboratory projects [13], and (3) purposefully designed virtual digital forensic environments, such as the *Cyber Sleuth Science Lab*³⁷ and the *CYber DEfenSe Trainer (CYDEST)* virtualized training platform for network defense and computer forensics [5].

Simulation can be utilized in digital forensic teaching in a variety of forms, from simulating how to seize a computer to presenting evidence as an expert witness in a simulated court room [11]. In contrast to face-to-face role playing in which students and tutors take on roles, virtual worlds created for digital forensics teaching provide role playing that may utilize bots (avatars animated by scripts) and image capture to add actual photos to the simulation, plus students can replay a particular scenario while taking on different roles, and educators can reuse modules across scenarios [10].

*CyberBit Range*³⁸ is a cybersecurity training and simulation platform with hyper-realistic scenarios, which features, among other things, network forensics, Windows forensics, and Linux forensics training. Cyberbit provides a sample course and workshop syllabi, which includes an example schedule for training cybersecurity forensics analysts. This schedule covers networking and communications, operating systems, network security and authentication, cyber-terminology and basics, vulnerabilities, malware and hacking, the Cyber Kill Chain, the anatomy of a cyberattack, data, databases, and logging, forensic tools, infection forensics, range simulation (SQL injection, killer Trojan, DDOS Syn flood, Java NMS kill, Trojan data leakage), machine forensics, network forensics, Linux, Linux forensics, practice scenario, espionage and data breaches, and infection prevention and remediation. This 6-week training was designed for first-time analysts, has two test preparation workshops, and a 2-part certification test. Considering its duration, the training's topics and schedule could be used when developing a curriculum for an accelerated online course on digital forensics.

Virtual reality (VR) labs for teaching digital forensics, such as *BMT ENGAGE*,³⁹ provide comparable learning outcomes to students learning the same material in physical labs, but with more time efficiency [15]. Immersive VR labs designed for this purpose can cover both concepts and hands-on laboratory exercises, such as bagging and tagging a virtual crime scene with digital devices.

3 Challenges of Teaching Digital Forensics

The main challenges of teaching digital forensics can be summarized by the various facets as follows:

³⁷ <https://www.cybersleuthlab.org>

³⁸ https://go.cyberbit.com/cyber_security_training-platform/

³⁹ <https://youtu.be/vBF-F3gXjfc>

- Technological challenges
 - *Size considerations*: authentic case studies require relatively large digital forensic image files (e.g., to demonstrate the physical acquisition of multi-terabyte SSDs/HDDs) that are difficult to ingest even locally, let alone in VMs using nested virtualization in a cloud environment. However, without these, the lecturer might end up using Mickey Mouse/toy examples.
 - *Bootable vs. not bootable VMs*: fully acquired drive volumes that are bootable as a VM can be authentic-looking and very useful for teaching, however, they constitute much larger digital forensic image files than logically acquired volumes that contain only selected parts of a volume. In addition, if a full acquisition is done to an actual physical drive, booting it may result in activating malware, which can infect other connected media.⁴⁰
- Legal challenges
 - *Authenticity*:⁴¹ it is tricky to generate case study files mimicking an illegal activity without actually performing that activity. One solution is a segregated computing environment, but creating one of these to mimic an enterprise-grade infrastructure is extremely complex and resource- and time-consuming, and many enterprise-grade networking hardware device cannot be virtualized/emulated.
 - *Licensing*: one of the primary questions for digital forensic training VMs is how to distribute them among students without violating copyright laws (e.g., a legal copy of Windows is not supposed to be cloned in VMs; would a free Linux distro solve this).
- Administrative challenges
 - *Plagiarism detection in repeating contents*: providing a document template with section titles to the students for writing a digital forensic investigation plan or a subsequent digital forensic investigation report might result in very high similarity scores on *Turnitin*.⁴²
 - *Self-explanatory and sufficient/complete descriptions*: create documentation for (overseas) facilitators and tutors can be very demanding as many intricacies of a digital forensic case study might be known only by the developer(s) unless a very comprehensive documentation is created, which might take longer to write than generating a dataset or making up the persons and devices of a hypothetical investigative case study.

⁴⁰ Booting into a VM based on a forensically sound image of a volume of a drive of a suspect's computing device changes some files, and operating system files in particular, every time the VM is booted, making the image content altered compared to the original volume content.

⁴¹ While real-world datasets are desirable for testing forensic tools for effectiveness and efficiency, they typically lack the ground truth that is vital for performing proper evaluations; in contrast, synthetic datasets can be purposefully generated for specific digital forensic tasks [38].

⁴² <https://turnitin.com>

- Pedagogical challenges
 - *Assessment size and complexity*: how to set the right balance between too easy and too complex, and how to set the right size (e.g., for exactly half a semester) is not trivial.
 - *Adding noise*: to create real world-like scenarios, additional challenges/non-trivial traces/misleading information also have to be included in case studies (e.g., encrypted drive, password-protected file, inconsistent event timestamps).
 - *Assessment alignment with the learning material*: creating links with the week-by-week tutorial materials can be very challenging when using an authentic-looking case study for an assignment, because the logical discussion of the digital forensics field consists of materials for teaching hands-on skills that are linked to pieces or facets of a case study that are absolutely not proportional, are not in a particular order, and the analysis of which rely on various levels of background knowledge, experience, and skills in different areas of computing and information security.
 - *Setting a good example*: demonstrating what can be done with various digital forensic tools might be tempting for some students, but it is important not to encourage nefarious online behavior by giving ideas, and ultimately, to teach students about professional and ethical behavioral practices in digital forensic investigations, and the consequences of not applying these. In addition, unintentional changes or destruction of artifacts (incl. potentially admissible evidence) can be devastating in digital forensic firms, and as such, should be prevented via correctly training best practices, such as using write blockers and never working on original media but on forensically sound copies of these.

4 Summary

The hands-on and interdisciplinary nature of digital forensics poses many challenges for teaching this field in tertiary settings, and these are not limited to technical challenges. However, some of these can be effectively overcome by utilizing unconventional teaching practices and technology-enhanced learning. Virtualized computing environments and simulated case study scenarios can accommodate efficient learning processes, enabling students to reach unit learning outcomes. However, creating these are time-consuming for educators, requires substantial resources, while even the most meticulously designed and documented digital forensic case study datasets can only be used in a couple of classes (to prevent collusion in assignments) and for a short period of time (due to technology obsolescence).

References

1. Allegra E, Pietro RD, Noce ML, Ruocco V, Verde NV (2011) Crossborder co-operation and education in digital investigations: A European perspective. *Digital Investigation* 8(2):106.113, <https://doi.org/10.1016/j.diin.2011.09.001>
2. Angelopoulou O, Vidalis S (2014) An academic approach to digital forensics. *Journal of Information Warfare* 13(4):57.69, URL <https://www.jstor.org/stable/26487467>
3. Antunes M, Rabadao C (2018) Cybersecurity and digital forensics – course development in a higher education institution. In: Madureira AM, Abraham A, Gandhi N, Silva C, Antunes M (eds) *Proceedings of the Tenth International Conference on Soft Computing and Pattern Recognition (SoCPaR 2018)*, Springer, Cham, pp 338–348, https://doi.org/10.1007/978-3-030-17065-3_34
4. Armstrong CJ (2007) An analysis of computer forensic practitioners perspectives on education and training requirements. In: Futcher L, Dodge R (eds) *Fifth World Conference on Information Security Education*, Springer, Boston, pp 1–8, https://doi.org/10.1007/978-0-387-73269-5_1
5. Brueckner S, Guaspari D, Adelstein F, Weeks J (2008) Automated computer forensics training in a virtualized environment. *Digital Investigation* 5S:S105–S111, <https://doi.org/10.1016/j.diin.2008.05.009>
6. Cahyani NDW, Martini B, Choo KKR, Ashman H (2018) An approach to enhance understanding of digital forensics technical terms in the presentation phase of a digital investigation using multimedia presentations. In: Beyah R, Chang B, Li Y, Zhu S (eds) *Security and Privacy in Communication Networks*, Springer, Cham, pp 488–506, https://doi.org/10.1007/978-3-030-01704-0_28
7. Cigoj P, Bla.i. BJ (2015) An innovative approach in digital forensic education and training. In: Bishop M, Miloslavskaya N, Theocharidou M (eds) *Information Security Education Across the Curriculum*, Springer, Cham, pp 101–110, https://doi.org/10.1007/978-3-319-18500-2_9
8. Craiger P (2008) Training and education in digital evidence. In: Barbara JJ (ed) *Handbook of Digital and Multimedia Forensic Evidence*, Humana Press, pp 11.22, https://doi.org/10.1007/978-1-59745-577-0_2
9. Craiger P, Burke P, Marberry C, Pollitt M (2008) A virtual digital forensics laboratory. In: Ray I, Shenoj S (eds) *Advances in Digital Forensics IV*, Springer, Boston, pp 357–365, https://doi.org/10.1007/978-0-387-84927-0_28
10. Crellin J, Karatzoun S (2009) Simulation in digital forensic education. 3rd International Conference on Cybercrime Forensic Education and Training, Canterbury Christ Church University, URL <https://core.ac.uk/download/pdf/29577405.pdf>
11. Crellin J, Adda M, Duke-Williams E (2010) The use of simulation in digital forensics teaching
12. Furnell S, K M, Piper F, E C, H C, Ensor C (2018) A national certification programme for academic degrees in cyber security. In: Drevin L, Theocharidou M (eds) *Information Security Education . Towards a Cybersecure Society*, Springer, Cham, pp 133–145, https://doi.org/10.1007/978-3-319-99734-6_11
13. Ghafarian A (2018) Using kali linux security tools to create laboratory projects for cybersecurity education. In: Arai K, Bhatia R, Kapoor S (eds) *Proceedings of the Future Technologies Conference (FTC) 2018*, Springer, Cham, https://doi.org/10.1007/978-3-030-02683-7_25
14. Govan M (2016) The application of peer teaching in digital forensics education. *Higher Education Pedagogies* 1(1):57–63, <https://doi.org/10.1080/23752696.2015.1134198>
15. Hassenfeldt C, Jacques J, Baggili I (2020) Exploring the learning efficacy of digital forensics concepts and bagging & tagging of digital devices in immersive virtual reality. *Forensic Science International: Digital Investigation* 33S, <https://doi.org/10.1016/j.fsidi.2020.301011>
16. Huebner E, Bem D, Cheung H (2010) Computer forensics education – the open source approach. In: Huebner E, Zanero S (eds) *Open SourceSoftware for Digital Forensics*, Springer, Boston, pp 9–23, https://doi.org/10.1007/978-1-4419-5803-7_2

17. Irons A, Thomas P (2015) Problem based learning in digital forensics. *Innovation in Teaching and Learning in Information and Computer Sciences* <https://doi.org/10.11120/ital.2014.00013>
18. Irons AD, Stephens P, Ferguson RI (2009) Digital investigation as a distinct discipline: A pedagogic perspective. *Digital Investigation* 1(1–2):82.90, <https://doi.org/10.1016/j.diin.2009.05.002>
19. Jahankhani H, Hosseinian-far A (2014) Digital forensics education, training and awareness. In: Akhgar B, Staniforth A, Bosco F (eds) *Cyber Crime and Cyber Terrorism Investigator's Handbook*, Syngress, chap 8, pp 91–100, <https://doi.org/10.1016/B978-0-12-800743-3.00008-6>
20. Kessler GC (2007) Online education in computer and digital forensics: A case study. In: Sprague RH (ed) *40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, IEEE Computer Society, Los Alamitos, CA, USA, <https://doi.org/10.1109/HICSS.2007.407>
21. Kessler GC, Haggerty D (2008) Pedagogy and overview of a graduate program in digital investigation management. In: Sprague RH (ed) *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)*, IEEE Computer Society, Los Alamitos, CA, USA, <https://doi.org/10.1109/HICSS.2008.345>
22. Kessler GC, Haggerty DA (2010) An online graduate program in digital investigation management: Pedagogy and overview. *Journal of Digital Forensic Practice* 3(1):11–22, <https://doi.org/10.1080/15567280903357771>
23. Kessler GC, Hoag J (2008) The power of simple hands-on cyberforensics exercises: A guide for faculty. In: *Proceedings of the 12th Colloquium for Information Systems Security Education*, pp 20–25
24. Kessler GC, Schirling ME (2006) The design of an undergraduate degree program in computer & digital forensics. *Journal of Digital Forensics, Security and Law* 1(3):37–50, URL <https://commons.erau.edu/db-security-studies/29>
25. Kessler GC, Simpson R, Fry J (2008) Extending the multidisciplinary learning experience in digital forensics using mock trials. In: E (ed) *Proceedings of CFET 2008: 2nd International Conference on Cybercrime Forensics Education & Training*, URL http://works.bepress.com/gary_kessler/11/
26. Kiper JR (2017) Forensic education: Towards a digital forensics instructional framework. URL <https://www.sans.org/readingroom/whitepapers/bestprac/paper/37582>
27. Kummer N, Delémont O, Voisard R, Weyermann C (2022) The potential of digital technologies in problem-based forensic learning activities. *Science & Justice* pp 1–3, <https://doi.org/10.1016/j.scijus.2022.04.005>
28. Lang A, Bashir M, Campbell R, DeStefano L (2014) Developing a new digital forensics curriculum. *Digital Investigation* 11(Supplement 2):S76–S84, <https://doi.org/10.1016/j.diin.2014.05.008>
29. Palmer I, Wood E, Nagy S, Garcia G, Bashir M, Campbell R (2015) Digital forensics education: A multidisciplinary curriculum model. In: James JI, Breiting F (eds) *Digital Forensics and Cyber Crime*, Springer, Cham, pp 3–15, https://doi.org/10.1007/978-3-319-25512-5_1
30. Read H, Sutherland I, Xynos K, Drange T, Sundt E (2017) The impact of changing technology on international cybersecurity curricula. In: Tryfonas T (ed) *Human Aspects of Information Security, Privacy and Trust*, Springer, Cham, pp 518–528, https://doi.org/10.1007/978-3-319-58460-7_36
31. Sabeil E, Manaf ABA, Ismail Z, Abas M (2011) Trainees' competency based-assessment methods in cyber forensics education or training programmes – a review. In: Zain JM, bt Wan Mohd WM, El-Qawasmeh E (eds) *Software Engineering and Computer Systems*, Springer, Heidelberg, pp 517–526, https://doi.org/10.1007/978-3-642-22170-5_44
32. Sikos LF (2020) AI in digital forensics: Ontology engineering for cybercrime investigations. *WIREs Forensic Science* 3(3):e1394, <https://doi.org/10.1002/wfs2.1394>

33. Simon M, Slay J (2007) Forensic computing training, certification and accreditation: An australian overview. In: Fitcher L, Dodge R (eds) Fifth World Conference on Information Security Education, Springer, Boston, pp 105–112, https://doi.org/10.1007/978-0-387-73269-5_14
34. Stenvert M, Brown I (2018) Qualifications and skill levels of digital forensics practitioners in South Africa: An exploratory study. In: Kabanda S, Suleman H, Gruner S (eds) ICT Education, Springer, Cham, pp 345–361, https://doi.org/10.1007/978-3-030-05813-5_23
35. Stigall M, Choo KKR (2021) Digital forensics education: Challenges and future opportunities. In: Choo KKR, Morris T, Peterson G, Imsand E (eds) National Cyber Summit (NCS) Research Track 2021, Springer, Cham, pp 28.46, https://doi.org/10.1007/978-3-030-84614-5_4
36. Tmienova NP, Ilarionov OE, Ilarionova NM (2017) Exploring digital forensics tools in Cyborg Hawk Linux. In: Dodonov AG, Golenkov VV, Lande DV, Khadzhyonov W, Tsyganok VV, Snarskii AA (eds) Selected Papers of the XVII International Scientific and Practical Conference on Information Technologies and Security (ITS 2017), RWTH Aachen University, Aachen, pp 118.124, URL <http://ceur-ws.org/Vol-2067/paper17.pdf>
37. Yang W, Johnstone MN, Sikos LF, Wang S (2020) Security and forensics in the Internet of Things: Research advances and challenges. In: 2020 Workshop on Emerging Technologies for Security in IoT, IEEE, pp 12–17, <https://doi.org/10.1109/ETSecIoT50046.2020.00007>
38. Yannikos Y, Graner L, Steinebach M, Winter C (2014) Data corpora for digital forensics education and research. In: Peterson G, Sheno S (eds) Advances in Digital Forensics X, Springer, Heidelberg, pp 309–325, https://doi.org/10.1007/978-3-662-44952-3_21
39. Yasinsac A, Erbacher RF, Marks DG, Pollitt MM, Sommer PM (2003) Computer forensics education. IEEE Security & Privacy 1(4):15–23, <https://doi.org/10.1109/MSECP.2003.1219052>
40. Zhang X, Choo KKR (eds) (2020) Digital Forensic Education: An Experiential Learning Approach. Springer, Cham, <https://doi.org/10.1007/978-3-030-23547-5>