Overcoming the Challenges of Teaching Cybersecurity in UK Computer Science Degree Programmes

***Abstract*—This Innovative Practice Full Paper explores the diversity of challenges relating to the teaching of cybersecurity in UK higher education degree programmes, through the lens of national policy, to the impact on pedagogy and practice. An article published in the Harvard Business Review in August 2019 argued that *"Every Computer Science Degree Should Require a Course in Cybersecurity "*; in the UK, universities – alongside government, industry and professional engineering bodies – have been championing this over recent years, focusing on computer science and cognate undergraduate degrees programmes; one such professional body (BCS, The Chartered Institute for IT) has been mandating this in accredited undergraduate degree programmes since 2015. Delivering cybersecurity effectively across general computer science programmes presents a number of challenges related to pedagogy, resources, faculty and infrastructure, as well as responding to industry requirements.**

There is a serious demand for cybersecurity specialists, both in the UK and globally (estimates vary, but are always large and increasing); there is thus significant and growing higher education provision related to specialist undergraduate and postgraduate courses focusing on varying aspects of cybersecurity (for example, cryptography, computer security, networks, digital forensics, ethical hacking, etc). To make our digital systems and products more secure, all in IT need to know some cybersecurity thus, there is a case for depth as well as breadth; this is not a new concern, but it is a growing one. Computer science and cognate engineering disciplines are evolving to meet these demands – both at school-level, as well as at university – however, doing so is not without challenges. This paper explores the progress made to date in the UK, building on previous work in cybersecurity education and accreditation by highlighting key challenges and opportunities, as well as identifying a number of enhancement activities for use by the international cybersecurity education community. It frames these challenges through concerns with the quality and availability of underpinning educational resources, the competencies and skills of faculty (especially focusing on pedagogy, progression and assessment), and articulating the necessary technical resources and infrastructure related to delivering rigorous cybersecurity content in general computer science and cognate degrees.

Though this critical evaluation of an emerging national case study of cybersecurity education in the UK, we also present a number of recommendations across policy and practice – from pedagogic principles and developing effective cybersecurity teaching practice, challenges in the recruitment, retention and professional development of faculty, to supporting diverse routes into post-compulsory cybersecurity education (and thus, diverse careers) – to provide the foundation for potential replicability and portability to other jurisdictions contemplating related education and skills reform initiatives and interventions.

***Index Terms*—cybersecurity, computer science education, curricula, accreditation, UK**

I. Introduction

An article published in the Harvard Business Review in August 2019 argued that "*Every Computer Science Degree Should Require a Course in Cybersecurity*" [1]; in the UK, universities — alongside government, industry and professional bodies – have been championing this over recent years, focusing on computer science and cognate undergraduate degrees programmes. One professional body — BCS, The Chartered Institute for IT — has been mandating this in accredited undergraduate degree programmes since 2015 [2]. Delivering cybersecurity effectively across general computer science programmes presents a number of challenges related to pedagogy, underpinning educational resources, available skills and technical resources. This paper explores the progress to date, as well as a starting call to arms to the UK higher education sector by highlighting a number of future challenges and opportunities.

As part of its promotion of sustainability, the United Nations(UN) defines "*UN Sustainability Goal 9: Build resilient infrastructure, promote sustainable industrialization and foster innovation*" [3]. For our computing technology infrastructure to be resilient we need to maintain and enhance cybersecurity. To achieve that we need to grow cybersecurity knowledge. As such the enhancement of cybersecurity education contributes directly to enhancing sustainability. The failure to maintain software infrastructure has been brought home by the recent U.S. shortage of COBOL programmers [4]. [5] demolish the "security through antiquity" argument often used to defend the COBOL systems, with [6] reporting that the explanation why key data were not encrypted was "it is not feasible to implement on networks that are too old".

II. Pedagogic Principles

Though it is generally thought of as part of computing, cybersecurity is actually a multidisciplinary "subject", or, in the words of [7] a *meta-discipline*. This point has been made several times, e.g. in [8], who described integrating Criminal Justice and Political Science into the study of cybersecurity.

A. Academic skills

The academic skill sets that a good Chief Information Security Officer (CISO) should have, and therefore that a cybersecurity student should acquire, can be broken into three rough groupings.

- **Psychology:** While this paper would not necessarily go as far as PurpleSec, who claim [9] that "98% of cyber attacks rely on social engineering", it is quite clear that a very large proportion do: not least the attacks classified as "phishing", "spear-phishing" and "whaling". The technical skills required to go phishing are minimal: being able to write

  ```
  <a href="bad url">good url</a>
  ```

  generally suffices, and even that can be bought in or with a little bit of technical knowledge one of the many open source penetration testing tools can be repurposed to help automate the process (for example [10], [11]). Forging e-mail addresses is generally needed as well if the intent is to go spear-phishing. But the real skill comes in knowing what will get under people's radar.

  To defend against phishing, to inculcate good password habits[1] and much more depends on understanding, or at least following the advice of those who understand, the psychology of the user [14]. In particular it is important not to fall into the "users are the enemy" trap [15].
- **Managerial:** Clearly the CISO has to manage the team. But there is much more than that. The CISO has to be a team player within top management. The CISO is responsible for the Cybersecurity Incident Response Plan(CIRP). But [16] lists among its major flaws in CIRPs that they are "lacking organisational support and buy-in:
  - Plan sponsor lacks appropriate authority (e.g., Executive Leadership Team, CIO, CTO, CISO);
  - Incident stakeholders do not know the plan exists;
  - Was developed unilaterally by a single business unit;
  - Roles and responsibilities for non-technical teams are vague."

  All of these are managerial failings.
- **Technical:** there are of course many technical things that a CISO needs to be on top of. They feature in the list [17] of "10 Essential Elements for Success as an Information Security Professional" as "(6) Find your speciality; (7) Maintain your technical edge; (8) Constantly improve your methodologies".

  These technical skills tend to be the ones that a Computer Science Department is best at teaching, though even here there are challenges — see section III. One specific question is "how much cryptography need a security expert know". The classic answer is "enough not to be dangerously ignorant, and not enough to be dangerously knowledgeable", which is true but not helpful: see §VI-C.

B. Human skills

Besides the subject-specific skills mentioned above, there are also the human, or 'soft', skills. It could be argued (e.g. [18]) that these are underrated throughout computing education, but they are certainly necessary in cybersecurity. [19] stresses them for the CISO, but the same is true throughout the cybersecurity industry. See also [20] — a publication that may have some bias, but the message resonates with much the authors have heard, and agrees with the Wall Street Journals Cybersecurity Executive Forum [21]. Their list of "top five skills" is this.

1) Problem-solving;
2) Communication;
3) Analytical thinking;
4) Collaboration/teamwork;
5) Attention to detail.

A Computer Science Department would probably claim that it taught most of these. Certainly a BCS-accredited degree has to evidence teaching and assessment of the first four of these. Collaboration/teamwork, is a long-standing requirement for accreditation, despite some student preferences the students' for such work not to be included or assessed as part of their degree [22]. Generally, it can be challenging to engage students whole-heartedly in the development of these skills, especially as they are hard to assess in the rigorous way computer scientists (staff and students) are used to.

These skills are all areas most people could always improve. The extent to which the depth graduates evidence these skills, compared with industry's demands is common point of discussion with industrialists informally or more formally as department industry liaison committees / forums. These work ready skills have also been noted by employability reviews conducted in the UK [23], [24]. Notably the collaboration required in cybersecurity is generally part of a multi-function team, rather than the group software engineering activity that commonly is the response to the demand to teach group working. Similarly the problem-solving required is that of being faced with an underspecified problem: "it looks like we've been hacked", but with a vast amount of information, most of it irrelevant.

Some alternative approaches to this is described in section VI.

III. Developing effective cybersecurity teaching practice

What is the most appropriate way to teach cybersecurity? [25] highlights there are benefits from teaching this in a practical manner. Real world case studies can be employed [26], [27, e.g.]. Use can be made of guest lectures by industrialists to share practical insights and hence providing students with micro-exposure to the world of work is another positive contribution. One further approach is the inclusion of appropriate cybersecurity standards within the curricula.

The PCI DSS [28] is one such standard that has been used in precisely this manner. PCI DSS underpins all processing of credit/debit cards. Nevertheless, it is very rarely mentioned in generalist computer scientist courses. This would not matter so much if everyone handling payments data were sent by their employers on an effective PCI DSS course. However, the payments business is now so spread across websites, often run by small and medium enterprises (SME), or non-specialists.

[1] Whatever those might be: opinions vary and well-known pundits (e.g. [12]) will disagree with NIST's advice [13].

Even larger enterprises are not immune: [26] reports that the recent British Airways breach was caused by a failure to adhere to PCI DSS in website maintenance. Section VI-C describes one way to bring PCI DSS to life in an assignment.

Another way of adopting a more practical pedagogy is by teaching cybersecurity through the lens of hacking or the hacker curriculum [29]. Such an approach facilitates students to be more experimental and creative in their exploration of the discipline and can have corresponding benefits for their engagement. This approach is most commonly employed within specialist cybersecurity education rather than more mainstream computer science. As indicated previously in the context of 'phishing' the technical skills required to engage in penetration testing (or indeed "hacking") are not that sophisticated with the use of the available tools (further examples including [30], [31]) [2]. However to fully understand the tool set and use it ethically would typically require more time and assessment than many computing departments wish to commit to the inclusion of cybersecurity in a mainstream computer science programme.

IV. Challenges in the recruitment, retention and professional development of faculty

It is well known that cybersecurity skills are in short supply, in both industry [32] and academia [33], [34]. The demand for cybersecurity skills in industry makes it difficult for academia to attract academics with knowledge, practical experience, research background and academic aspirations. As universities expand their cybersecurity provision it is not uncommon to find multiple jobs advertised at the same time. Recent example have included a professor of cybersecurity, two senior academic positions and two junior academic positions in one advert. There are other examples in the UK of cybersecurity lecturing jobs remaining unfilled for longer than a year; there are also examples of cybersecurity research groups moving en masse from one university to another.

For example, research into the state of IT conducted annually by Enterprise Strategy Group (ESG) has revealed that the skills gap in information security continues to widen and has doubled in the past five years; in 2014, 23% of respondents to the survey stated that their organisation had a problematic shortage of information security skills – this had climbed to 51% at the beginning of 2018 [35]. The 2020 ESG report, does not quantify the skills gap in the same way, however does highlight the continued global cybersecurity shortage and that *"most organizations will increase cybersecurity spending in 2020...CISOs will spread budget dollars around in many areas."* [36, p.1]. Clearly, cybersecurity is an issue which is being felt across many industries and organisations, and is a concern which extends beyond IT leadership into the boardroom [32].

The ESG survey is international, but ESG have confirmed that the UK figures are very similar. In the UK, there has been a resurgence of job adverts to recruit academic staff with specialisms in cybersecurity over the past three years.

Cybersecurity is not a static field, and it is vital that the teacher keeps up-to-date. This is not necessarily easy, as developments such as the attacks on Zoom [37, etc.] show. Although [37] is largely technical, and the lawsuits [38, etc.] have been about this or managerial failings over privacy management, the problems in practice [39], [40] have largely been about user education and practices, and the human end of the interface. Hence the teacher, when asked "what do you make of the recent Zoom fuss" has to be capable of responding across all the academic areas (§II-A).

It cannot be emphasised too strongly (not least to Heads of Departments!) that this isn't just a "check the notes at the start of the year" exercise: during the writing of this paper, one author got an e-mail at 21:00 that caused him to rewrite the slides for the following morning's 09:00 lecture.

V. Quality of resources to support cybersecurity education?

Effective teaching requires appropriate supporting resources. The extent to which appropriate resources are available and suitable will be evaluated next. This evaluation highlights a number of occasions when underpinning resources could be improved.

A. Underpinning resources

The formal resources for Cybersecurity education are in reasonable shape given the inevitable fast-moving nature of the subject. The authors see [41] as a major work, though probably daunting as a textbook. It is dated, but a new edition is in preparation, and largely on the author's website. More recently a UK-funded project has produced the "Cyber Security Body Of Knowledge" [42]. This is not intended as a textbook, but is a useful reference.

One gap in the educational resources is the absence, as far as the authors know, of a good answer to "how much cryptography need a security expert know".

More worrying is the problem described in [2, §IV.B] — the state of general computer science educational resources with respect to cybersecurity. In particular [43] describes the poor state of database textbooks with respect to SQL injection. Despite the fact that SQL injection is theoretically well-understood, it is still a real problem today, twenty years after it was first described:

> Overall, SQL Injection (SQLi) accounted for more than 72of all attacks when looking at all verticals during this period [December 2017–November 2019]. [44]

B. Provision of laboratories

Delivering a practical take upon cybersecurity often requires specialist computing resources, certainly if any form of penetration testing/ethical hacking is to be taught. The traditional solution to this was a dedicated laboratory, generally not connected to the outside world (in the case of the UK,

[2]The tools are intended for penetration testing but can be readily repurposed.

the JANET network) in order not to breach the operating conditions of the network. In practice it will probably not even be directly connected to the university's internal network for the same reasons. An upmarket version of such a laboratory is described in [45], though an adequate one can be build for roughly £10,000 in capital costs. The real problem, which many computer science departments in the UK will struggle with, is the staffing to support the maintenance of such a facility. This in itself requires specialist cybersecurity skills, which are in short supply and universities in the UK at least are hardly renown for paying technical support staff high wages! Specialist teaching laboratories are challenging and time consuming to maintain: lost passwords, trashed machines if the hacking escapes, etc., and the problems of keeping the underlying infrastructure up-to-date with security patches while not changing the target machines the students are practising against.

An interesting alternative is to host such a laboratory "in the cloud", as recommended by, for example, [46]. This would eliminate the capital expenditure (in favour of recurrent cloud costs, but these should be significantly less). The impact on technician/support time is less clear. Ideally it ought to be less, but a lot depends on the extent to which the cloud provider's authentication structure can be interfaced with the host university's: the second author is currently having problems here with an unrelated piece of teaching outsourcing.

Outsourcing to the cloud means that the students' "hacking" commands traverse the university's and the external networks, even though then are not "commands" until they reach the laboratory in the cloud. Different universities in the UK, even reading the same external network's (JANET's) policies, have different views on whether this is permissible.

VI. Teaching Innovations

As introduced in section I, teaching cybersecurity well for the workplace is more than about academic skills. However, it is very hard to motivate computer scientists to study pure human skills. This is far from being a feature of students, as [47] observes.

> Still, technical knowledge seems to trump everything. I've attended national and regional information security conferences that have sessions on security careers and the essential soft skills for cybersecurity success. They're not nearly as well attended as the sessions on cool and sexy topics like threat hunting, cryptocurrency and ransomware.

Hence the ideal assignment in cybersecurity mixes the academic and human skills, preferably inseparably.

How Cybersecurity is being taught in university departments is evolving rapidly. A number of alternative approaches exist. In this section, examples are provided of teaching innovations that have been effective. The examples are far from an exhaustive list, instead are illustrative of some opportunities and alternative approaches with the intention of surfacing innovations that could be considered for wider exploitation.

A. Cybersecurity - inspiring potential students

Steganography is the art of hiding information in full view but its use pre-dates computers. For example, the ancient Greeks used to shave a slaves head, write a message on their skull and then allow the hair to grow before sending them on a journey to the receivers location [48]. Bringing this "secure transmission of data" into the modern era, it is possible use steganography approaches to, for example, hide data within an image and transmit the modified image to a receiver without anyone noticing that the image has been altered. It works by replacing the least significant bits of the colour of each pixel with the data you wish to transmit. Whilst this does change the colour of individual pixels, in say a full 24-bit image (where there is 1 byte for each of the red, green and blue components), the change is almost imperceptible, even when viewed side by side with the original image. Taking an image of 800x600 pixels, it is possible to "secretly" transmit 800*600 pixels * 3 bits of data or 180000 bytes.

This topic has been delivered as a "Masterclass" falling under promotion and recruitment activity for both local and international students. Given this activity occurs prior to enrolment, it has the benefit of raising the importance of security issues among potential computer science students at the outset of their careers, as well as raising awareness of those who show some interest in computing but who ultimately take up other career paths. It also allows the topic to be introduced in the context of fundamental computer science topics such as binary, programming (as an encoder and decoder are required) and how an image and indeed characters are represented within a computer. The talk also covers broader aspects such as what type of information needs to be transmitted securely, why it is important to be able to transmit information securely, the risks associated with people other than the intended recipient gaining access to the information and hence the need to consider cybersecurity issues when designing and developing computer systems. Introducing security issues in the context of these traditional topics, "mainstreams" them, and hence raises their perceived importance among "tomorrows students".

B. Approaches to including cybersecurity in general computer science

In general terms two alternatives approaches can be effectively adopted to the challenge of embedding cybersecurity in a general computer science degree:

1) Cybersecurity can be primarily delivered in a single course / module / subject and then referred to in other courses / modules/ subjects as appropriate.
   Or
2) The teaching and assessment can be distributed across the curricula.

The next two examples provide an example of each of these approaches.

C. Computer Science - embedding cybersecurity in a single module / subject

This example refers to, what in the UK is a medium sized computer science programme with an intake that has grown in recent years to between 100-120 students. In this example the approach adopted is to primarily deliver the cybersecurity content within a single subject / module and then signpost relevant cybersecurity issues in other subjects / modules as appropriate. The advantage of this is, cybersecurity becomes a significant curricula component, the importance of which is very visible to learners. However the downside, is that learners may be tempted to consider cybersecurity as a specialism, rather than something that should always be considered [49].

This Cybersecurity module is part of a general computing degree. As such there is a wide range of backgrounds on the course. In section II-A the question "how much cryptography need a security expert know" was posed. The answer for this course is "about 90 minutes worth", which seems to cover the bases well enough: for example enough time to enable cryptographic hashing to underpin the lecture on password management (which is not part of the 90 minutes).

Since Cybersecurity is a practical subject, much of the learning takes place through the coursework. The assessment for the module is structured with these weightings.

20 Class test — basically a traditional examination. Normally a closed-book test, but this year, due to Covid-19, it will be sat by students who have dispersed, so will have to be open-book.

30 Group presentation. The class divide themselves into groups of 4–5, and each group picks a topic from either the "OWASP Top 10" [50] or the "OWASP Mobile Top 10" [51] and does a presentation on it to the rest of the class. In terms of the human skills identified in section II-B, this is meant to help with the communication and team-working skills. Indeed, Covid-19 and the consequent dispersal of the students has meant that they are also learning remote team working: an unexpected bonus. During the delivery, it has found that it is extremely important to share this rationale, and the evidence at [20], [21], [47] with the student community. Industrial speakers are also asked to stress these points.

50 The students have to analyse three different (i.e. different vendors and style) on-line purchases (or mock-purchases, they are allowed to use an invalid credit card) made subject to PCI DSS, looking at the screen as the ordinary customer would see it, but also at the browser logs (HAR files) and network logs (Wireshark or equivalent). For each, they are asked the following.

1) With which websites does your browser communicate during the transaction? Are there any that worry you, or whose function you do not understand?
   * Last year two different students, purchasing from two different UK-based sites, found `yandex.ru` appearing here.
2) Looking at the logs, to which sites does your payment card number get sent, and how is it protected in transit? You *should* quote the relevant part of the logs, but *should* replace the card number and any other identifying/sensitive data, e.g. by `NNNN NNNN NNNN NNNN`, before quoting.
3) Looking at the HTML(+JavaScript etc.) you have saved, do you feel confident you know what it is doing with your data?
4) How dependent is the HTML you have on the correct functioning of the DNS? In particular, could bad DNS results result in a security problem?
5) What makes you think that the sum of money displayed to you is the sum that will be transmitted to your bank?

Question 4 is meant to help students realise the interconnected nature of today's Internet, and the hidden dependencies. A lecture related to DNS has always been part of this course, but this year the recent wave of home router attacks [52, and others] was included. This illustrates the fact that cybersecurity is always throwing up new examples and illustrations, which can be good for student motivation, but sets a real challenge for the teacher in terms of keeping up to date.

In addition, they are asked these overall questions.

1) What have you learned about the security of your card data?
2) In particular, what did you learn from the logs/HTML that you could not have reasonably deduced as a shopper with no access to these?
3) How obvious is the security of the websites to the shopper?
4) How might the system be more transparent to the shopper?

Questions 3 and 4 are really open-ended "problem-solving" questions, to which the author doesn't have a neat solution. This really frustrates students, who want to know "the right answer", but is much closer to reality.

D. Computer Science - embedding cybersecurity across the curricula

This example relates to teaching Cybersecurity to general computer science undergraduate students at university in the United Kingdom . The programme has an intake of about 240 students. The students upon the programme study a foundation of computer science for the first two years of their study before specialising in Internet of Things, Web Development, Games Development or Artificial Intelligence. This generic structure is fairly typical of Computer Science degree programmes delivered in the United Kingdom.

Rather than have a module dedicated to cybersecurity the teaching and assessment of the cybersecurity is embedded across the curricula as shown in Table I. The rationale for this is, cybersecurity becomes integral and learners are encouraged to consider cybersecurity as something that should always be

considered as part of normal practice. The consequence is that none of the individual modules/subjects or their related assessments are entirely related to cybersecurity (e.g. In an exam, a few questions will be cybersecurity related rather than the whole examination). If this is evaluated pessimistically, then learners could consider cybersecurity as a peripheral issue, however experience of the approach indicate this has not been the case.

The approach taken is to emphasise the practical dimension of cybersecurity for the benefits advocated by [25]. To this end a Visiting Industrial Professor has been employed to support the viewpoint of industry in the design, delivery and assessment of the programme of study. The Visiting Industrial Professor is a senior industrialist specialising in cybersecurity and supports the department for 12 days of the academic year. During this time, the Visiting Industrial Professor advises upon context, develops and delivers classes, mentors students with interests in security careers and provides developmental support to academic colleagues. Student satisfaction questionnaires have been employed related to each of the interactions with students delivered by the Visiting Industrial Professor and whilst the completion rate remains low (less than 10 percent of the cohort, responses remains universally popular.) So not only is the use of a Visiting Industrial Professor ensuring the Cybersecurity content is industrially relevant, it is also popular with students. A third benefit of this approach, is the inclusion of cybersecurity has a very visible champion who raises awareness within the academic staff base, supports Continued Professional Development (CPD) of academics and helps ensures the cybersecurity is appropriately taught and assessed within the syllabus.

As can be seen from Table I, cybersecurity is integrated across the syllabus. The large cohort of students studying the programme has quite a diverse range of interests.

Significant use of project work is made within the curricula. When project work is completed,as much as possible students choose the subject/area of the project they undertake. The rationale is to harness learner creativity [53] and hence enhance the students' engagement with their studies. Projects possible are limited by an appropriate set of constraints. In the context of the first year Systems Analysis module, teams of students engage in a research activities to establish the scope of a system of their choosing. All projects are subject to university ethical approval which constrains the projects to those which are appropriate and achievable. A wide variety of systems are explored including games, web applications, mobile applications and so on. As part of this process students are required to explore and document the personal, organisation and legal/regulatory framework in which the system selected can be used, including risks and constraints related to its cybersecurity. The Industrial Professor, assists in briefing students and provides guidance on the general personal, organisation and legal/regulatory framework. Additionally, the Industrial Professor, is available to discuss the specific context of cybersecurity within the chosen projects. This is an important curricula area, however one in which it is challenging to gain high student engagement. However this approach of mixing creativity with industry insights does appear to motivate learning.

In the final year of their studies, all the students complete a team project with the Team Project and Professionalism subject. In this subject teams of students develop a software product of their own choosing. This is typically related to their chosen specialism. These projects must be *"live"*, normally addressing the needs of a real client but always addressing a real problem [3]. A variety of products are developed for example games, web applications, mobile applications, wearable applications, computational intelligence solutions, IoT prototypes and so on. Teams of students are required to develop and then demonstrate a prototype application. This work forms a capstone to students studies and student are required to share their development via GitHub. They are encouraged to consider the work as a career portfolio element which in turn helps to evidence their capabilities to future employers. The produced prototype and its future potential commercial exploitation are evaluated. The produced prototype, is expected to address personal, organisation and legal/regulatory framework in which the system they have selected can be used, including risks and constraints related to its cybersecurity. If there are limitations in this regard the students are expected to be abreast of them. Also, as part of this evaluation students are expected to evaluate the personal, organisation and legal/regulatory framework of the potential future exploitation of the project, including risks and constraints related to its cybersecurity. Similar guidance and support is provided by the visiting Industry Professor for the Team Project and Professionalism subject that was provided to System Analysis student, although it is in more depth and sophisticated insights are expected (as well as evidence from the practical development work).

As indicated, part of the rationale of this approach is to harness student creativity and hence raise engagement with the studies. As the assessment is divergent [54] (students are all completing different projects), the assessment reduces the opportunity to engage in academic misconduct as there would be little to be gained from fellow students work. The integrative manner in which cybersecurity is consider and considering as part of the capstone also raises the importance that students view cybersecurity. The rationale is to promote cybersecurity as something that needs to be always considered, not an optional extra. Feedback from students indicates, this emphasis upon building secure systems is of interest to employers and a common discussion point during employment interviews. Hence the appointment of the Visiting Industrial Professor is of benefit to academic staff, students and their future employers. It is also of benefit to the Visiting Professor as enables them to participate as an equal partner in an academic environment and hence gain valuable CPD.

[3]A minority of students use the project to prototype a product they are considering using in a future business venture and a small number of other students address a research problem in collaboration with a university research group. However all projects involved the creation of a software product.

TABLE I
CYBER SECURITY CURRICULA COVERAGE CASE STUDY §VI-D

Subject / Module	Year	Taught	How Assessed
Web Technologies	1	Confidentiality, integrity and availability. Threats and Attacks, how they materialise and how those attacks exploit website vulnerabilities.	Web page providing user training related to cybersecurity.
Systems Analysis	1	Personal, organisation and legal/regulatory framework in which a system can be used, including risks and constraints.	Self selected team Design Project
Databases	1	Threats and Attacks, how they materialise and how those attacks exploit database vulnerabilities.	Examination questions
Web Programming	2	Threats and Attacks, how they materialise and how those attacks exploit web vulnerabilities and approaches to mitigate.	A web application, secured again OWASP top ten vulnerabilities
Programming Design and Development	2	Design, defensive programming and testing	Programming project and related report
Networks, Operating Systems and Cybersecurity	2	Cybersecurity architecture and operations: physical and process controls that can be implemented across an organisation to reduce information and systems risk, identify, and mitigate the vulnerability, and ensure organisational compliance	Practical work and related report
Team Project and Professionalism	3	Personal, organisation and legal/regulatory framework in which a system can be used, including risks and constraints.	Design and construction of a software component as part of a self selected team project and the evaluation of the project and its potential future exploitation. The projects are 'live' addressing the needs of a real client or problem.

The team project based nature of both these modules has been adopted to facilitate the development of the students Human Skills (§II-B). As in §VI-C, this year Covid-19 and the consequent dispersal of the students has meant that they are also learning remote team working: an unexpected bonus. Appropriate academic skills (§II-A) are evidenced partly in the manner the practical work is completed but also in the case of the final year Team Project and Professionalism module by the quality and content of the evaluative report.

E. Delivering specialist Cybersecurity degrees

This example refers to the delivery on dedicated BSc and MSc courses in Cybersecurity. The insights shared have been gained in experience of delivering specialist cybersecurity degree programmes since 2005 at several universities. During this time a number of assessment instruments in cybersecurity to encourage students to use the assessment activities to enable student learning, described more fully in [blinded]. The use of scenarios to encourage students to think both as attackers and defenders has been particularly helpful in enabling students to understand the cybersecurity environment. As an overall assessment strategy in cybersecurity attempts should be made to:

- get students to identify and critically evaluate threats ranging from nuisance threats to advanced persistent threats;
- design, develop and implement strategies to counter the threats;
- identify when breaches or attacks have taken place and critically evaluate the impact of those;
- design, develop and implement approaches to recover from attack;
- give students the opportunity to evaluate attacks and develop more robust cybersecurity defences as a result.

The above can be done in the context of specific cybersecurity scenarios or case studies, but can also be utilised to encourage students to think about and present policies and procedures for cybersecurity environments.

One particularly effective assessment which helps pull together many of the cybersecurity threads and complexities is the use of "infographs". An extract from an assessment using infographs is given below.

> The cybersecurity environment is a wide and complex one. For the first part of this assignment you are required to produce an infograph (1 page) outlining the typical threats that either a) individuals in society or b) organisations face from breaches of cybersecurity. The design of your infograph and the content of the infograph is left to you to decide but you should consider visual impact, key messages, data to support, examples and underpinning research. You will have the chance to present your infograph to your peers, academics and guests from industry. You should be able to discuss the points raised on your infograph, explaining the detail and answering any questions asked.

As well as allowing the student to analyse and evaluate a particular issue or concern the assessment enables the development and assessment of a series of professional competencies (see section II-B), including communication, presentation skills, and the summarising of complex cybersecurity issues.

VII. CONCLUSIONS AND FURTHER WORK

In the previous section, we seen some examples in which the delivery of cybersecurity has been enhanced. The approaches emphasise the need for both the academic and human skills, and also that there isn't a "one size fits all" approach.

On the practical side, the community could do much to help itself in the way of sharing best practice.

1) Given the shortage of staff in the area (section §IV), and the fact that universities have to teach this with less-than-ideally qualified staff, there is a real need for coordinated professional development in this area.
2) For cybersecurity content to be effectively included in general computer science programmes it has to be led. This can be effectively achieved by including a specialist module / subject related to the area or it can be effectively achieved on a cross curricula basis providing the inclusion is appropriately led / championed. There is an opportunity to consider employing part time visiting industrial professor to do precisely this. This may help address some of the issues related to shortage of staff (§IV).
3) Including input from cybersecurity professionals (as guest lectures or in other ways) is well received by student communities and should form a recommended practice for the impact is has related to raising engagement, promoting employability and enhancing the curricula.
4) Cybersecurity can be seen to be enthusing and exciting potential students, this represents an opportunity to potentially extend and diversify the student basis as well as an opportunity to promote knowledge of cybersecurity issues in the wider community. This is also a challenge to the teacher, who must be constantly refreshing the stock of examples to stay current.
5) Sharing good practice with respect to physical laboratories, especially reducing technical support effort.
6) The same for in-cloud laboratories.
7) At least in the UK, getting university lawyers to form a consistent view on the legitimacy of outsourcing cybersecurity laboratories to the cloud.
8) There are a number of innovative and effective practices emerging related to the teaching and assessment of cybersecurity. There is an opportunity for the computer science educational community to engaging in further cataloguing and dissemination of these approaches.

ACKNOWLEDGEMENT

Removed for blind refereeing.

REFERENCES

[1] J. Cable, "Every computer science degree should require a course in cybersecurity," Aug 2019. [Online]. Available: https://hbr.org/2019/08/every-computer-science-degree-should-require-a-course-in-cybersecurity

[2] T. Crick, J. Davenport, A. Irons, and T. Prickett, "A UK Case Study on Cybersecurity Education and Accreditation," in *Proc. IEEE Frontiers in Education Conference*. USA: IEEE, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/9028407

[3] UN, "Goal 9:Sustainable Development Knowledge Platform," https://https://sustainabledevelopment.un.org/sdg9, 2020.

[4] E. Shein, "COBOL programmers are in demand to fight the coronavirus pandemic," https://www.techrepublic.com/article/cobol-programmers-are-in-demand-to-fight-the-coronavirus-pandemic/, 2020.

[5] M.-S. Pang and H. Tanriverdi, "Security Breaches in the U.S. Federal Government (March 7, 2017)," 2017. [Online]. Available: https://weis2017.econinfosec.org/wp-content/uploads/sites/3/2017/05/WEIS_2017_paper_52.pdf

[6] A. Sternstein, "Heated House Hearing Offers New Clues Into How Hackers Broke Into OPM Networks," 2015. [Online]. Available: https://www.nextgov.com/cybersecurity/2015/06/heated-house-hearing-offers-new-clues-how-hackers-broke-opm-networks/115474/

[7] A. Parrish, J. Impagliazzo, R. K. Raj, H. Santos, M. R. Asghar, A. Jøsang, T. Pereira, and E. Stavrou, "Global perspectives on cybersecurity education for 2030: a case for a meta-discipline," in *Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*, 2018, pp. 36–54.

[8] M. Stockman, "Infusing social science into cybersecurity education," in *Proceedings of the 14th Annual ACM SIGITE Conference on Information Technology Education*, ser. SIGITE 13. New York, NY, USA: Association for Computing Machinery, 2013, pp. 121–124. [Online]. Available: https://doi.org/10.1145/2512276.2512302

[9] PurpleSec LLC, "The Ultimate List Of Cyber Security Statistics For 2019," https://purplesec.us/resources/cyber-security-statistics, 2020.

[10] Jordan Wright, "Open-Source Phishing Framework," https://getgophish.com/, 2020.

[11] E. Daguerre, B. Geise, J. McCutchan, and S. McIntyre, "Phishing Campaign Toolkit," https://github.com/rsmusllp/king-phisher, 2020.

[12] R. Grimes, "The best password advice right now (Hint: It's not the NIST guidelines)," https://www.csoonline.com/article/3306757/the-best-password-advice-right-now.html, 2019.

[13] National Institute for Standards and Technology, "NIST Special Publication 800-63B: Digital Identity Guidelines: Authentication and Lifecycle Management," https://pages.nist.gov/800-63-3/sp800-63b.html, 2019.

[14] P. Inglesant and M. Sasse, "The true cost of unusable password policies: password use in the wild," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2010, pp. 383–392.

[15] A. Adams and M. Sasse, "Users are not the enemy," *Commun. ACM*, vol. 42, no. 12, pp. 40–46, 1999.

[16] Secureworks, "5 Common Questions Asked of Our Incident Responders," *Secureworks Inc.*, 2019. [Online]. Available: https://www.secureworks.com/resources/wp-incident-response-common-questions

[17] K. Beaver, "RSA Tips for CISOs: From 10 Years Ago to Today," https://securityintelligence.com/rsa-tips-for-cisos-from-10-years-ago-to-today/, 2017.

[18] S. Palkar, "Industry-academia collaboration, expectations, and experiences," *ACM Inroads*, vol. 4, no. 4, pp. 56–58, 2013.

[19] A. Froehlich, "What is the role of CISO in network security?" 2019. [Online]. Available: https://searchsecurity.techtarget.com/answer/What-is-the-role-of-CISO-in-network-security

[20] Infosec Institute, "5 soft skills you need to be a successful security pro," 2019. [Online]. Available: https://resources.infosecinstitute.com/security-pro-5-soft-skills/

[21] Wall Street Journal, "Cybersecurity Requires 'Insatiable' Problem-Solving Skills; Technical Skills Can Be Taught," https://blogs.wsj.com/cio/2018/05/24/cybersecurity-requires-insatiable-problem-solving-skills-technical-skills-can-be-taught/, 2018.

[22] T. Crick, J. Davenport, P. Hanna, A. Irons, and T. Prickett, "Computer Science Degree Accreditation in the UK: A Post-Shadbolt Review Update," *CEP 2020: Proceedings of the 4th Conference on Computing Education Practice*, 2020.

[23] N. Shadbolt, "Shadbolt review of computer sciences degree accreditation and graduate employability," https://www.gov.uk/government/publications/computer-science-degree-accreditation-and-graduate-employability-shadbolt-review, 2016.

[24] W. Wakeham, "Stem degree provision and graduate employability: Wakeham review," https://www.gov.uk/government/publications/stem-degree-provision-and-graduate-employability-wakeham-review, 2016.

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

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

[27] Zoom Blog (Oded Gal), "The Facts Around Zoom and Encryption for Meetings/Webinars," https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/, 2020.

[28] Payment Card Industry Security Standards Council (PCI SSC), "Requirements and Security Assessment Procedures Version 3.2.1," 2018. [Online]. Available: https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss

[29] S. Bratus, A. Shubina, and M. E. Locasto, "Teaching the principles of the hacker curriculum to undergraduates," in *Proceedings of the 41st ACM technical symposium on Computer science education*, ACM. USA: ACM, 2010, pp. 122–126.

[30] O. S. Limited, "Kali Linux: Penetration Testing and Ethical Hacking," https://www.Kali.org/, 2020.

[31] Rapid7, "MetaSploit: The worlds most used penetration testing framework," https://www.metasploit.com/, 2020.

[32] R. Ackerman, "Too few cybersecurity professionals is a gigantic problem for 2019," https://techcrunch.com/2019/01/27/too-few-cybersecurity-professionals-is-a-gigantic-problem-for-2019/, 2019.

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

[34] B. E. Endicott-Popovsky and V. M. Popovsky, "Searching and developing cybersecurity talent," in *Journal of The Colloquium for Information System Security Education*, vol. 5, no. 2, 2018, pp. 17–17.

[35] ESG, "2018 Cybersecurity Spending Trends," https://www.esg-global.com/research/esg-brief-2018-cybersecurity-spending-trends, 2018.

[36] ——, "2020 Cybersecurity Spending Trends," https://www.esg-global.com/research/esg-brief-2020-cybersecurity-spending-trends, 2020.

[37] B. Marczak and J. Scott-Railton, "Move Fast & Roll Your Own Crypto: A Quick Look at the Confidentiality of Zoom Meetings," https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/, 2020.

[38] J. Dame, "Zoom privacy: Vendor faces lawsuits over Facebook data-sharing," https://searchunifiedcommunications.techtarget.com/news/252480965/Zoom-privacy-Vendor-faces-lawsuit-over-Facebook-data-sharing, 2020.

[39] L. Abrams, "Over 500,000 Zoom accounts sold on hacker forums, the dark web," https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web/, 2020.

[40] A. Culafi, "Zoom takes new security measures to counter 'Zoombombing'," https://searchsecurity.techtarget.com/news/252481257/Zoom-takes-new-security-measures-to-counter-Zoombombing, 2020.

[41] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems (second edition)*. Wiley, 2008.

[42] University of Bristol Cyber Security Group, "The Cyber Security Body Of Knowledge: Issue 1.0," https://www.cybok.org/, 2019.

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

[44] Akamai Ltd., "Financial Services — Hostile Takeover Attempts," *Akamai state of the internet Security*, vol. 6, no. 1, 2020.

[45] R. T. Abler, D. Contis, J. B. Grizzard, and H. L. Owen, "Georgia tech information security center hands-on network security laboratory," *IEEE Transactions on Education*, vol. 49, no. 1, pp. 82–87, 2006.

[46] K. Salah, "Harnessing the cloud for teaching cybersecurity," in *Proceedings of the 45th ACM technical symposium on Computer science education*, 2014, pp. 529–534.

[47] K. Beaver, "The must-have skills for cybersecurity aren't what you think," https://searchsecurity.techtarget.com/opinion/The-must-have-skills-for-cybersecurity-arent-what-you-think, 2019.

[48] Herodotus, *The Histories*. Manuscript, BC 440.

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

[50] Open Web Application Security Project (OWASP), "The Ten Most Critical Web Application Security Risks," https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=Main, 2017.

[51] ——, "Mobile Top 10 2016-Top 10," https://wiki.owasp.org/index.php/OWASP_Mobile_Top_10#tab=Top_10_Mobile_Risks, 2016.

[52] N. Balaji, "Hackers Hijack Home Routers & Change The DNS Settings to Implant Infostealer Malware," https://gbhackers.com/hackers-hijack-home-routers-dns-settings/, 2020.

[53] S. Bradley, "Creative assessment in programming: Diversity and divergence," in *Proceedings of the 4th Conference on Computing Education Practice 2020*, ser. CEP 2020. New York, NY, USA: Association for Computing Machinery, 2020. [Online]. Available: https://doi.org/10.1145/3372356.3372369

[54] ——, "Managing plagiarism in programming assignments with blended assessment and randomisation," in *Proceedings of the 16th Koli Calling International Conference on Computing Education Research*, ser. Koli Calling 16. New York, NY, USA: Association for Computing Machinery, 2016, p. 2130. [Online]. Available: https://doi.org/10.1145/2999541.2999560