https://doi.org/10.1080/19361610.2020.1798173

Cyber Security Index For Undergraduate Computer Science Courses in the UK

[1]Natasha Ruiz, [2] Dr Pancham Shukla, [2] Prof Hassan Kazemian

[1]PhD candidate, School of Computing and Digital Media, London Metropolitan University / CTI Renato Archer-DIMEC, Rodovia Dom Pedro I (SP-65), Km 143,6 - Campinas, SP, Brazil- ORCID[0000-0003-1644-3933]

[2] School of Computing and Digital Media, London Metropolitan University

***Abstract*: The paper proposes a novel index to classify how well UK Computer Science courses articulate cybersecurity related content through their course/module pages. The aim of this work is to raise awareness among British Universities to pay more attention to include and standardise cyber security content in computer science courses. Our results show that 80% of analysed courses scored 1 or 2-stars on a 5-Stars scale. The results also suggest the need of a formal delivery of cybersecurity content from the first year of the courses and possibly in a collaborative manner with the British Computer Society (BCS). To emphasize cybersecurity education in mitigating security lapses, the analogy is: it is better if most people know how to use a match than to train many fire-fighters.**

Keywords: Cybersecurity Index, Computer Science, Undergraduate, Human Factors, Cyber Security Education, IT Education

I. INTRODUCTION

As reported in [1], we have two technological features threatening the global economy for the first time in a decade: i) cyber attacks and ii) data fraud. These two are within the top five most likely global risks such as natural disasters, extreme climate events and the failure to mitigate climate change. Technological threats are now recognized as an important theme and represent the first step towards improving security in cyberspace.

People are at the centre of all technology developments and their uses. Human factors do influence technological features and hence are the principal issues in this context. According to [2], understanding the requirements for the regional, national or accredited cyber security programs are necessary to ensure that there are identified benchmarks that are applied and are being met.

In USA, the National Security Agency (NSA) gives accreditation to Cyber Security courses that use the National Initiative for Cyber Security Education (NICE) Framework [3]. However, this is only for specific Cyber Security courses. In our research, we did not find similar accreditations for computer science courses, coherently, across a range of Universities globally.

In line with Higher Education Statistics Agency (HESA) [4], there were 79,480 students enrolled on Computer Science courses in the UK in 2016/17. Whether UK undergraduate students are being prepared to develop cyber secure programs for the society was investigated in [5]. To do this, the authors analysed the curricula of UK computer science courses.

This work proposes a creation of an index to classify UK Universities by the relevance with which each institution offers cybersecurity content in their computer science courses. We didn't look specifically at cybersecurity courses. Rather, this work analyses the 'preparedness' of UK undergraduate students who are expected to develop software that meet baseline cybersecurity standards through their G400 courses [6].

II. LITERATURE REVIEW

A list of countries that plan to include compulsory learning of Computer Science in secondary education, highlights how this discipline is being taught at an increasingly earlier age. This list includes Austria, Australia, Finland, France, Germany, Ireland, Italy, Japan, Lithuania, Portugal, Republic of Korea, South Africa and Spain [7].

The European Commission has published a report that proposes three levels of knowledge on cybersecurity each student needs to know. These levels are: beginner, intermediate and advanced [8].

If the aim is to teach secure programming to the youngsters, it´s necessary to make sure the future teachers of Computer Science are being prepared during their undergraduate courses and learn how to teach their future pupils about secure software development.

Conforming to Professors Moufida Sadok and Peter Bednar, an excessively technical focus is one of the main reasons why there are deficiencies in cybersecurity [9]. If technology is only a part of the problem, why does society pay so much attention to the technical side of the problem?

> "While information security risks have involved and financial costs of cybercrime have increased, security practices and strategies have not adequately kept up with

> dynamic and challenging attacks that are highly complex and difficult to detect." [9]

Conversely, are security problems caused by the high costs of maintaining security?

Human factors are discussed by [10] and this work presents two cases on security incidents caused by human factors in two financial organizations. It also mentions the relevance of education in information security.

Privacy and cybersecurity issues and the pleaded (alleged?) solutions offered by software vendors [11] [12] [13] [14] [15] raise doubts about vendors' promises. The privacy as advertised is hardly provided. Typically, they recommend the developers to explicitly alert the users of their products on the limitations of private browsing functionality. These papers testify how relevant the human factors are in the realm of the cybersecurity.

Surveys such as one carried out by the DSS Company [16] are very common and normally highlight special product features. Moreover, manufacturers often exaggerate what their solutions offer in terms of efficient protection and sometimes beyond the scope of achievable security. Parallelly, knowing and exploiting these loopholes, hackers continue to attack vulnerable and high-profile institutions.

According to statistics from the Russian information security certification system, about one-third of the pieces of software tested exhibited vulnerabilities during a two-year study. According to [17], [18] and [19], it´s not known how failures can compromise information security and people's privacy.

It is possible to confirm that attackers can gain full access to encrypted files, enabling credentials previously revoked, including TrueCrypt [20], VeraCrypt [21], GhostCrypt [22] and PGP Symantec Encryption Desktop [23].

When a trainee configures TrueCrypt or similar software for a business person, politician, high-ranking military or a researcher, installing the piece of software with the password "123", the user is advised to change it to a "strong password" and share the password [24] [25] [26].

Personal credentials enter the e-commerce domain when a user buys flowers, food, vehicles and company-shares on the New York Stock Exchange, or takes part in home banking to pay bills and/or to make other bank transactions. When majority of common users are affected internationaly, the scale is of global proportion.

The research in this field focuses on the treatment of user login information (usernames and passwords) by major service provider websites such as search sites, home banking, e-mail and e-commerce. In these cases, the focus is how clients input important personal details, and how these websites manage their users' passwords.

In terms of security attacks, in Existential Forgery, an attacker can forge an authenticator for some unspecified user [27], which means that he/she cannot target one specific user. Whereas in Total Break, an attacker can recover the user key and can, therefore, build valid authenticators at his/her will.

As mentioned in [28], it´s important to analyse a vast class of information on the navigation activities that browsers save onto the hard-disk. Credentials were found in the form of clear text in non-volatile memory. This occurred with all browsers tested by the author of the mentioned paper. Independent of the browser, Gmail, Amazon, eBay, Hotmail, and the Santander, Caixa and Citibank websites showed the similar vulnerability [29].

Investigations into cryptographic programs, web browsers and web credentials have shown that the credential management, security and privacy protection measures are currently quite poor. Meanwhile, investigations into "in-private navigation" show that the "privacy software" does not, in fact, gives adequate privacy to the user. Many researchers have focused on the technological aspects of the cases such as flaws in the code written or project errors. But, if vendors and users continue to manage credentials the way they are doing, it cannot be more vulnerable than a locked car with the car-key left in the door-lock. What can one expect from cybersecurity and privacy when many users and organisational practises are relaxed in protecting personal credentials?

> "We use TrueCrypt in a corporate/enterprise environment. Is there a way for an administrator to reset a volume password or pre-boot authentication password when a user forgets it (or loses a key file)? Yes. Note that there is no 'back door' implemented in TrueCrypt. However, there is a way to 'reset' volume passwords/key files and pre-boot authentication passwords." [26]
>
> "If someone needs to access an encrypted file or a shared encrypted laptop, the encryption password will need to be shared, unlike your University password which should always be kept private. If you forget the encryption password for a file or USB stick, then the data will be inaccessible. In the case of laptops encrypted by the University, IT Services will store a recovery disk that will enable the laptop password to be reset." [24]

In the same way when universities orient their pupils and users towards using "in-private" navigation, one has to stand still and review what is being taught about security and privacy [30] [31].

In [32], cybersecurity is classified in four categories: public, infrastructure, business and general. The basic message is to transform cybersecurity courses in a multidisciplinary direction. While this is laudable, broadening the knowledge of security experts do not solve the issue.

> "From a socio-technical perspective, it is claimed that a viable system would be more user-centric by accommodating and balancing human process rather than entertaining an expectation of a one-sided change of behaviour of the end-user." [9].
>
> "Two reasons could potentially explain the poor effectiveness of the implemented security solutions and procedures: the boundary problem of risk analysis scope and the background of involved actors in risk assessment and security policy design." [9]

Sadok and Bednar's the work considers human-centricity as the best approach to address the cybersecurity problems.

It´s necessary to adjust the whole background, specifically, the way cybersecurity and privacy are explained to the students. It proposes five units for High School programming courses in Israel: fundamentals, advanced programming, second paradigm, applications and theory. Likewise, [33] declares that security is among the key aspects in the field of computing.

Twenty-two years after the latter study, an interesting piece of research carried out in the US about teaching Computer Science in High School has suggested a new curriculum for teaching programming to teenagers [34]. Unfortunately, no security or privacy aspects have been considered so far.

In United States the national Centres of Academic Excellence in Cyber Defense Education (CAE-CDE) works with NSA to improve criteria to elevate the quality of cyber security education [35]. It presents three case studies of different institutions with different CAE statuses highlighting the importance of the CAE designation in enhancing cybersecurity education at these institutions. Unfortunately, all these studies and initiatives are about specialized cyber security undergraduate courses designed to prepare cyber security specialists.

In New Zealand, there have been discussions about Computer Science on the High School curriculum, albeit, without taking cybersecurity and privacy into account [35].

In the UK, researchers have been concerned with teaching Computer Science to produce more and more programming from the secondary level onwards [36] [37] [38].

> "The challenge of introducing security in a sensible and useful manner can be addressed by considering the contextual perspectives". [9]

However, the basis of cybersecurity must be introduced in early education, according to the Joint Task Force on Cybersecurity Education [39]. While this report provides guidelines for delivering cybersecurity education, all managers of technological courses could benefit from reading it.

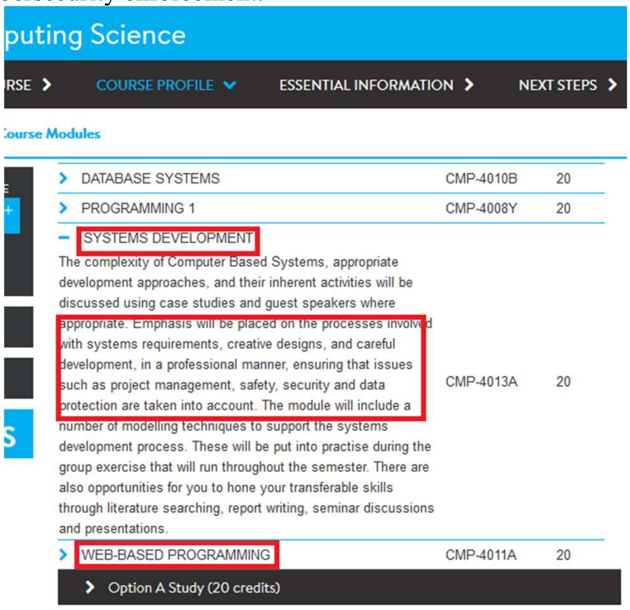
The focus of our work is to suggest an index that demonstrates how cybersecurity is taught in Computer Science (G400) courses in the UK with the aim to emphasize its relevance and to foster improvement initiatives in the University curricula.

III. METHOD AND DATA COLLECTION

From the perspective that everything has a human element, the authors gathered information to understand what UK universities are thinking about cybersecurity and how students on relevant courses are being trained. For this, it was necessary to analyse the curricula of the offered courses. For that, it was decided to study the common basis of relevant course, disregarding cybersecurity specific courses. In particular, to understand the depth and breadth of cyber security related topics and their application, authors found Computer Science courses quite appropriate.

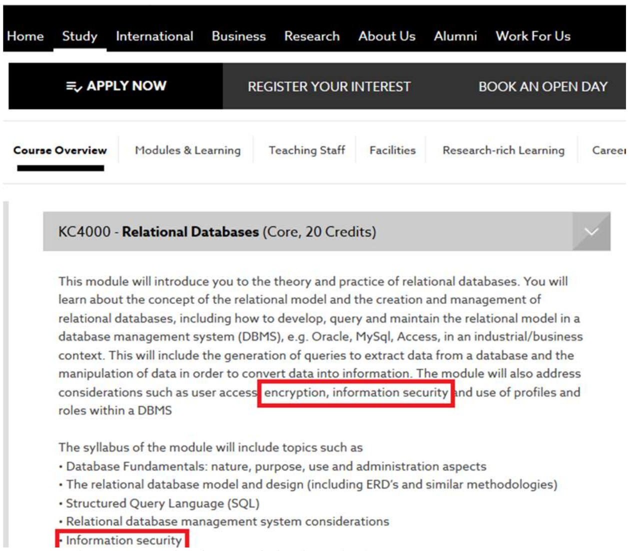
The authors considered the discipline components of 100 G400 Computer Science or similar courses [6], from the top 100 UK universities offering such courses as selected by the ranks in "Webometrics Ranking of World Universities" - an initiative of the Cybermetrics Lab- a research group belonging to the *Consejo Superior de Investigaciones Científicas* (CSIC) being one of the largest public research body in Spain [41]. This ranking includes 280 UK universities. This study considers that the first 100 UK universities representing a sizable sample of the UK universities that offer some cybersecurity related content on their Computer Science or related courses

The title of the module or discipline and the content of the discipline as seen on Fig.1, Fig.2 and Fig3., when available online, were manually read line by line to identify cybersecurity content keywords such as security, privacy, cybersecurity, risk management, forensics, cryptography, safe software, safe programming, cybercrime, data protection, credential management and others security terms or expressions, or other contextualized elements that refer to cybersecurity enforcement.



DATABASE SYSTEMS	CMP-4010B	20
PROGRAMMING 1	CMP-4008Y	20
SYSTEMS DEVELOPMENT The complexity of Computer Based Systems, appropriate development approaches, and their inherent activities will be discussed using case studies and guest speakers where appropriate. Emphasis will be placed on the processes involved with systems requirements, creative designs, and careful development, in a professional manner, ensuring that issues such as project management, safety, security and data protection are taken into account. The module will include a number of modelling techniques to support the systems development process. These will be put into practise during the group exercise that will run throughout the semester. There are also opportunities for you to hone your transferable skills through literature searching, report writing, seminar discussions and presentations.	CMP-4013A	20
WEB-BASED PROGRAMMING	CMP-4011A	20

Fig. 1 One of the best module descriptions founded.

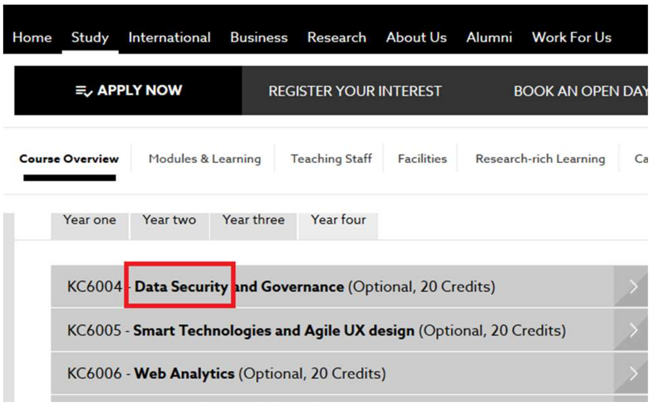


KC4000 - **Relational Databases** (Core, 20 Credits)

This module will introduce you to the theory and practice of relational databases. You will learn about the concept of the relational model and the creation and management of relational databases, including how to develop, query and maintain the relational model in a database management system (DBMS), e.g. Oracle, MySql, Access, in an industrial/business context. This will include the generation of queries to extract data from a database and the manipulation of data in order to convert data into information. The module will also address considerations such as user access encryption, information security and use of profiles and roles within a DBMS

The syllabus of the module will include topics such as
- Database Fundamentals: nature, purpose, use and administration aspects
- The relational database model and design (including ERD's and similar methodologies)
- Structured Query Language (SQL)
- Relational database management system considerations
- Information security

Fig. 2 Security content in the module description.



KC6004 - **Data Security and Governance** (Optional, 20 Credits)

KC6005 - **Smart Technologies and Agile UX design** (Optional, 20 Credits)

KC6006 - **Web Analytics** (Optional, 20 Credits)

Fig. 3 Security content in the module title.

If a word or expression linked to security was found during the reading of a discipline's menu, it was scored as summarized in Table 1.

Annotations were made by the authors to identify at which point in time the security element was addressed, as well as whether the subject discipline was mandatory or optional.

The proposed Index of Relevance in Cyber Security (IRCS) privileges the mandatory content and the content given at the beginning of the course. The higher the mandatory content and the higher the content in the first year of the course, the higher the IRCS index as given by:

$$\mathbf{IRCS} = \sum MC * 1 + \sum OC * 0.2 + \sum FYC * 1 + \sum SYC * 0.3 + \sum LYC * 0.15$$

Where,
MC = Mandatory content;
OC = Optional content;
FYC=First year content;
SYC=Second year content;
LYC=Latest year content.

Table 1-Collected data extracted by reading course descriptions provided by each institution on their website and classified by IRCS.

				Year		
IRCS	**University**	**OC**	**MC**	**FYC**	**SYC**	**LYC**
9,2	Robert Gordon University	0	8	0	0	8
5,1	University of Winchester	1	3	1	3	0
4,6	University of Liverpool	0	4	0	0	4
3,65	Lincoln University	1	2	1	1	1
3,45	Bangor University	0	3	0	0	3
3,45	University of Portsmouth	0	3	0	0	3
3,3	De Montfort University	0	2	1	1	0
3,3	University of Bedfordshire	0	2	1	1	0
3,15	University of Bradford	0	2	1	0	1
2,65	University of Kent	1	2	0	0	3
2,6	University of Derby	0	2	0	2	0
2,45	University of Reading	0	2	0	1	1
2,45	Edge Hill University	0	2	0	1	1
2,3	University of Oxford	0	2	0	0	2
2,05	University of Plymouth	5	0	0	2	3
2	University of Central Lancashire	0	1	1	0	0
2	Bournemouth University	0	1	1	0	0
2	London Metropolitan University	0	1	1	0	0
2	University of Abertay	0	1	1	0	0
2	University of Sunderland	0	1	1	0	0
1,9	Bristol University	3	0	1	0	2
1,9	Staffordshire University	3	0	1	0	2
1,65	University of Birmingham	1	1	0	1	1
1,65	University of Salford	1	1	0	1	1
1,5	University of Leeds	1	1	0	0	2
1,5	University of Ulster	1	1	0	0	2
1,5	University of Hertfordshire	1	1	0	0	2
1,4	University of Stirling	4	0	0	0	4
1,3	University of Cambridge	0	1	0	1	0
1,3	University of Exeter	0	1	0	1	0
1,3	Oxford Brookes University	0	1	0	1	0
1,3	University of Huddersfield	0	1	0	1	0
1,3	University of South Wales (Glamorgan & Wales Newport)	0	1	0	1	0
1,3	Teesside University	0	1	0	1	0
1,3	Birmingham City University (University of Central England)	0	1	0	1	0
1,2	Keele University	1	0	1	0	0
1,15	King's College London	0	1	0	0	1
1,15	Lancaster University	0	1	0	0	1
1,15	Aston University	0	1	0	0	1
1,15	Goldsmiths University of London	0	1	0	0	1
1,15	University of East London	0	1	0	0	1
1,15	London South Bank University	0	1	0	0	1
1,15	Cardiff Metropolitan University (University of Wales Institute Cardiff)	0	1	0	0	1
1,05	Loughborough University	3	0	0	0	3
1,05	Brunel University	3	0	0	0	3
1,05	City University London	3	0	0	0	3
0,7	Imperial College London	2	0	0	0	2
0,7	University of Southampton	2	0	0	0	2
0,7	Newcastle University Newcastle upon Tyne	2	0	0	0	2
0,7	University of Sheffield	2	0	0	0	2
0,7	Cardiff University	2	0	0	0	2
0,5	Kingston University London	1	0	0	1	0
0,35	University of Manchester	1	0	0	0	1
0,35	University of Warwick	1	0	0	0	1

0,35	University of Nottingham	1	0	0	0	1
0,35	Queen Mary University of London	1	0	0	0	1
0,35	University of Leicester	1	0	0	0	1
0,35	University of Saint Andrews	1	0	0	0	1
0,35	University of Surrey	1	0	0	0	1
0,35	Queen's University Belfast	1	0	0	0	1
0,35	The University of the West of England	1	0	0	0	1
0,35	Manchester Metropolitan University	1	0	0	0	1
0,35	University of Chester	1	0	0	0	1
0	University College London	0	0	0	0	0
0	University of Edinburgh	0	0	0	0	0
0	University of Glasgow	0	0	0	0	0
0	Durham University	0	0	0	0	0
0	University of York	0	0	0	0	0
0	University of Aberdeen	0	0	0	0	0
0	University of East Anglia	0	0	0	0	0
0	University of Sussex	0	0	0	0	0
0	University of Bath	0	0	0	0	0
0	University of Strathclyde	0	0	0	0	0
0	Heriot-Watt University	0	0	0	0	0
0	University of Essex	0	0	0	0	0
0	Swansea University	0	0	0	0	0
0	Royal Holloway University of London	0	0	0	0	0
0	Aberystwyth University / Prifysgol Aberystwyth	0	0	0	0	0
0	Cranfield University	0	0	0	0	0
0	Birkbeck University of London	0	0	0	0	0
0	University of Hull	0	0	0	0	0
0	Northumbria University	0	0	0	0	0
0	University of Brighton	0	0	0	0	0
0	Sheffield Hallam University	0	0	0	0	0
0	Liverpool John Moores University	0	0	0	0	0
0	Nottingham Trent University	0	0	0	0	0
0	University of Greenwich	0	0	0	0	0
0	Middlesex University	0	0	0	0	0
0	Coventry University	0	0	0	0	0
0	University of Westminster	0	0	0	0	0
0	University of Wolverhampton	0	0	0	0	0
0	Glasgow Caledonian University	0	0	0	0	0
0	Anglia Ruskin University	0	0	0	0	0
0	Napier University Edinburgh	0	0	0	0	0
0	Leeds Beckett University (Leeds Metropolitan University)	0	0	0	0	0
0	Canterbury Christ Church University	0	0	0	0	0
0	University of Bolton	0	0	0	0	0
0	University of Gloucestershire	0	0	0	0	0
0	University of Northampton	0	0	0	0	0
0	University of Worcester	0	0	0	0	0

IV. DISCUSSION

For simplicity, one may cluster (or group) the courses given in Table 1 on a 5-Stars scale as follows:

1 Star = IRCS <1
2 Stars = IRCS between 1 to 1,99
3 Stars = IRCS between 2 to 2,99
4 Stars = IRCS between 3 to 3,99
5 Stars= IRCS >= 4

54% of courses – 1 Star
26% of courses – 2 Stars
11% of courses – 3 Stars
6% of courses – 4 Stars
3% of courses – 5 Stars

In this work, we attempted to examine how well UK students on computer Science courses are exposed to mandatory cybersecurity content at the beginning of the course.

The apparent absence of anything about security and privacy in the curricula says a lot about the relevance of this theme on the courses in question. If cybersecurity content is not written into the discipline's syllabus, it is likely that it won't be taught formally and the consequences of this are potentially disastrous as emphasized in the literature review.

The heuristic analysis indicates that more than one-third of G400 courses in the UK leave cybersecurity as their mandatory curricula leaving cybersecurity as an optional discipline.

The first stage in the process of acquiring knowledge is to "remember" [44]. To remember something, one needs to be exposed to something new at an early stage with reinforced exposure carefully planned for the set duration.

Reflecting on [10], people are at the centre of any technological design and as mentioned by the author of [42], the education of cybersecurity content seems to be failing to attend the societal needs.

V. CONCLUSION AND FUTURE WORK

Based on our novel IRCS index for the sourced dataset, we concur to [46] [5] [44] in the sense that the best manner to make cyberspace safer is to teach cybersecurity to Computer Science students from the first year of the University as a mandatory content.

It is very desirable and important to have an evolved and more objective IRCS index to effectively measure the cybersecurity content in the Computer Science curricula. As a future work, we would like to derive robust IRCS by enhancing Table 1 with other scores such as professional certification or accreditation liked to the course. In addition, we would like to automate the scoring with exhaustive keywords that can fully encompass the course and module webpages.

VI. REFERENCES

[1] World Economic Forum, “Global Risks Report 2018,” World Economic Forum, Geneva, 2018.

[2] M. Dawson, “Hyper-connectivity: Intricacies of national and international,” *Doctoral Thesis at London Metropolitan,* 2017.

[3] D. Shoemaker, A. Kohnke and K. Sigler, The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit), Boca Raton: CRC Press, 2016.

[4] HESA, “Higher Education Statistics Agency: UK, 2016/17,” HESA, Promenade, 2018.

[5] R. Ruiz, “A Study of the UK Undergraduate Computer Science Curriculum: A Vision of Cybersecurity,” in *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, London, 2019.

[6] Universities Central Council on Admissions, “Universities Central Council on Admissions,” 2018. [Online]. Available: https://www.ucas.com/ucas-terms-explained. [Accessed 01 February 2018].

[7] D. Passey, “Computer science (CS) in the Compulsory Education Curriculum: Implications for Future research,” *Education and Information Technologies,* vol. 22, p. 401, 2017.

[8] A. Ferrari, “DIGCOMP: A Framework for Developing and Understanding Digital Competence in Europe,” European Commission Institute for Prospective Technological Studies, Seville , 2013.

[9] M. Sadok and P. Bednar, “Understanding Security Practices Deficiencies: A Contextual Analysis. In S. Furnell, & N. Clarke (Eds.),” in *Human Aspects of Information Security and Assurance Conference Proceedings*, Plymouth , 2015.

[10] A. Reza and H. J. a. A. A.-N. Shareeful Islam, “Analyzing Human Factors for an Effective Information Security Management System,” *International Journal of Secure Software Engineering (IJSSE),* vol. 4, no. 1, pp. 50-74, 18 9 2013.

[11] R. d. S. Ruiz, F. P. Amatte and K. J. B. Park , "Opening the “Private Browsing” Data – Acquiring Evidence of Browsing Activities," in *Proceedings of the International Conference on Information Security and Cyber Forensics*, Kuala Terengganu, Malaysia, 2014.

[12] R. Ruiz, K. Park, F. Amatte and R. Winter, "Overconfidence: Personal Behaviors Regarding Privacy that Allows the Leakage of Information in Private Browsing Mode," *International Journal of Cyber-Security and Digital Forensics (IJCSDF),* vol. 4, no. 3, pp. 404-416, 2015.

[13] R. d. S. Ruiz, F. P. Amatte and K. J. B. Park, "Tornando Pública a Navegação “InPrivate”," in *Proceedings of the IcoFCS2012*, Brasília - Brazil, 2012.

[14] G. B. E. J. C. B. AGGARVAL, “An Analysis of Private Browsing Modes in Modern Browsers,” in *Proceedings of the USENIX 2010*, 2010.

[15] R. Ruiz, R. Winter, K. Park and F. Amatte, Apoc@lypse: The end of antivirus, North Charleston: North Charleston: CreateSpace Independent Publishing Plataform, 2015, p. 134.

[16] A. Filatov, “Data Security Solution,” 25 02 2015. [Online]. Available: http://pt.slideshare.net/AndSor/dss-symantec-pgp-encryption-fortress2014-arrowecs-roadshow-baltics.

[17] R. d. S. Ruiz, F. P. Amatte and K. J. B. Park, "Security Issue on Cloned TrueCrypt Containers and Backup Headers," in *The International Conference on Cyber-Crime Investigation and Cyber Security (ICCICS2014)*, Kuala Lumpur - Malaysia, 2014.

[18] R. Winter and R. Ruiz, “Corrosive Secrecy and Confidence: The Paradox Among Bypassing Cryptographic Software, Loss of Privacy and Information Security,” *Cyber Security Review,* pp. 66-74, 01 03 2016.

[19] R. Ruiz and R. Winter, “Lazarus: Data Leakage with PGP and Resurrection of the Revoked User,” *Journal of Cyber Security and Mobility,* vol. 5, no. 2, pp. 1-14, 20 11 2016.

[20] T. Foundation, “Truecrypt,” 15 02 2013. [Online]. Available: http://truecrypt.org.

[21] IDRIX, “VeraCrypt,” 2018. [Online]. Available: https://veracrypt.codeplex.com/.

[22] Ghostcrypt, “Ghostcrypt,” 04 01 2018. [Online]. Available: https://www.ghostcrypt.org/.

[23] Symantec, “Symantec Desktop Encryption User Manual,” [Online]. Available: https://symwisedownload.symantec.com/resources/sites/SYMWISE/content/live/DOCUMENTATION/6000/DOC6205/en_US/symcEncrDesktop_103_win_usersguide_en.pdf?__gda__=1475850268_90925006947a919661523e2f67f5cea7. [Accessed 5 October 2016].

[24] IT Services, The University of Manchester,, “Encryption Software,” 2014. [Online]. Available: http://www.itservices.manchester.ac.uk/cybersecurity/advice/encryption/.

[25] University of Exeter, “Important Information for Users of TrueCrypt on Windows Laptops,” 25 April 2014. [Online]. Available: http://www.exeter.ac.uk/ig/infosec/encryptionforlaptops/usingtruecrypt/.

[26] Wake Forest University, “TrueCrypt install,” 25 04 2014. [Online]. Available: http://users.wfu.edu/yipcw/is/truecrypt/.

[27] K. S. K. F. N. FU, “Dos and Don'ts of Client Authentication On The Web,” in *Proceedings of the 10th USENIX Security Symposium*, Whashington DC, 2001.

[28] J. L. S. L. S. Oh, “Advanced Evidence Collection and Analysis of Web Browser Activity,” *Digital Investigation,* pp. 62-70, 2011.

[29] R. Ruiz, R. Winter, K. Park and F. Amatte, “The leakage of passwords from home banking sites: A threat to global cyber security?,” *Journal of Payments Strategy and Systems,* vol. 11, no. 2, pp. 174-186, 2017.

[30] University of Michigan, “Safe Computing,” 01 September 2018. [Online]. Available: https://www.safecomputing.umich.edu/be-aware/privacy/resources.

[31] Wake Forest University School of Business, “MSBA Software Installation,” 2018. [Online]. Available: business.wfu.edu/msba-software.

[32] R. B. Ramirez, Making Cyber Security Interdisciplinary: Recommendations for a Novel Curriculum and Terminology Harmonization, Cambridge: Master’s thesis in technology and policy, Massachusetts Institute of Technology, 2017.

[33] J. Gal-Ezer, C. Beeri, D. Harel and A. Yehudai, “A High-School Program in Computer Science,” *Computer,* vol. 28, no. 10, pp. 73-80, 1995.

[34] G. Alexandron, M. Armoni, M. Gordon and D. Harel, “Teaching Scenario-based Programming: An Additional Paradigm for the High School Computer Science Curriculum, Part 1,” *Computing in Science & Engineering,* vol. 19, no. 5, pp. 58-67, 2017.

[35] P. Wang, M. Dawson and K. L. Williams, “Improving Cyber Defense Education Through National Standard Alignment: Case Studies.,” in *National Security: Breakthroughs in Research and Practice, edited by Information Resources*, Management Association, IGI Global, 2019, pp. 78-91.

[36] T. Bell, P. Andreae and L. Lambert, “Computer Science in New Zealand High Schools,” Brisbane, 2010.

[37] N. C. C. BROWN, S. SENTANCE, T. CRICK and S. HUMPHREYS, “Restart: The Resurgence of Computer Science in UK Schools,” *ACM Transactions on Computing Education (TOCE),* vol. 14, no. 2, p. 9, 2014.

[38] N. C. C. Brown, M. Kölling, T. Crick, S. P. Jones, S. Humphreys and S. Sentance, “Bringing Computer Ccience Cack Into Schools: Lessons From The UK,” Denver, 2013.

[39] S. Sentance, M. Dorling, A. McNicol and T. Crick, “Grand challenges for the UK: upskilling teachers to teach computer science within the secondary curriculum,” Hamburg, 2012.

[40] ACM; IEEE-CS; AIS SIGSEC; IFIP WG 11.8, “Cybersecurity Curricula 2017,” ACM; IEEE-CS; AIS SIGSEC; IFIP WG 11.8, New York, 2017.

[41] Cybermetrics, “Webometrics,” 2018. [Online]. Available: http://www.webometrics.info. [Accessed 04 02 2018].

[42] B. (. E. M. F. E. H. W. K. D. Bloom, Taxonomy of Educational Objectives, Handbook I:, Allyn & Bacon ed., New York: Pearson, 1956.

[43] J. M. Pittman and R. E. Pike, “An Observational Study of Peer Learning for High School Students at a Cybersecurity Camp,” *Information Systems Education Journal,* vol. 4, no. 3, pp. 4-13, 13 5 2016.

[44] N. Ruiz, P. Shukla and H. Kazemian, “Privacy in The First Line of the First Code,” 17 04 2020. [Online]. Available: https://science.sciencemag.org/content/317/5842/1178/tab-e-letters. [Accessed 27 04 2020].