A Study of the UK Undergraduate Computer Science Curriculum: A Vision of Cybersecurity

Rodrigo Ruiz
Centro de Tecnologia da Informação Renato Archer
45 PUBLICATIONS **37** CITATIONS

Paper accepted at 12th International Conference on Global Security, Safety & Sustainability 2019, London

A Study of the UK Undergraduate Computer Science Curriculum: A Vision of Cybersecurity

Rodrigo Ruiz[0000-0003-1644-3933]

DICSI/NSSI

CTI Renato Archer, Rodovia Dom Pedro I (SP-65), Km 143,6 - Campinas, SP, Brazil - ZIP 13069-901

rodrigosruiz@outlook.com

Abstract: **When the content is not written in the discipline syllabus, it is possible that it will not be taught. In this work, the author has investigated 100 computer science undergraduate courses in the UK, to assess the capability of the software developers in the Country to create secure pieces of software. Besides that, to evaluate to which extent the UK Engineering and System Design students are being taught about the relevance of considering security issues when developing software or if this subject is treated as just an optional element at the end of their professional education.**

Keywords: Cybersecurity; Computer Science; Undergraduate; Human Factors; Teaching; I.T. Education.

I. INTRODUCTION

According to the *Global Risk Report 2018* [1], for the first time in a decade, we have two technological features threatening the global economy: cyberattacks and data fraud being the top five most likely global risks, abreast with natural disasters, extreme climate events and the failure to mitigate climate change. Recognizing such technological threats is important and represents the first step towards improving security in cyberspace.

Considering that people develop all technology, human factors are the principal issue in the context of abusive communications and faulty software since the 1970s.

Moreover, the technology is not the main cause of data leakage. Sometimes, users are influenced by sophisticated marketing campaigns, that reaffirm the quality of products and services.

If cybersecurity is on the international agenda, it makes sense to ask whether our people are prepared to tackle this topic. According to HESA [2], there were 79,480 students enrolled on Computer Science courses in the UK in 2016/17. This work investigates whether UK graduate students are being prepared to develop secure programs for the society. In order to do this, the author has analysed the curricula of UK computer science courses.

It´s worth mentioning that this work is not looking specifically at cybersecurity courses. Professionals working in this field are rather as firefighters who extinguish flames in buildings (or, in this case, into the cyberspace) made according to security standards. Rather, this work analyses the education of UK students who are responsible for developing software based on cybersecurity standards.

II. LITERATURE REVIEW

Some years ago, computers were operated by highly specialized people in data processing offices. Today, many educators and politicians think that all of our children need to know computer programming. A list of countries that plan to include compulsory learning on Computer Science in secondary education or under, highlight how the encompassed disciplines are 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 [3].

When one thinks about teaching computer programming to children and adults he/she must consider how they will be educated to develop secure software. The European Commission has published a report that proposes levels of knowledge about cybersecurity, suggesting what each student needs to know in three phases: beginner, intermediate and advanced levels [4].

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 to learn how to teach their future pupils about secure software development. It´s to say, how one can design a piece of software, taking into account since the very beginning, security concerns.

According to Professors Moufida Sadok and Peter Bednar, an excessively technical focus is one of the main reasons why there are deficiencies in cybersecurity [5]. If technology is only a part of the problem, why does society pay only and too 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.” [5]

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

Human factors are discussed by [6] and they work present two cases on security incidents caused by human factors in two financial organizations, also mentioning the relevance of education in information security. [6]

A careful assessment of the current actual privacy and cybersecurity issues and the pleaded/alleged solutions offered by software vendors, [7] [8] [9] [10] raises doubts about vendors' promises. The privacy as advertised is not provided. Typically, they recommend the developers to explicitly alert the users of their products about the limitations of private browsing functionality.

Moreover, cybercriminals are capable enough toclone passwords from Internet users. A survey conducted by Insight Express and Cisco [11] draws attention of the IT professional' perceptions about data loss incidents in companies and gives solid supporting arguments reinforcing the importance of protecting companies' sensitive information:

> "70% of IT professionals believe the use of unauthorized programs responds for as many as half of their companies 'data loss incidents'." [11]
>
> "44% of employees share work devices with others without supervision." [11]
>
> "39% of IT professionals said they have dealt with an employee accessing unauthorized parts of a company's network or facility." [11]
>
> "46% of employees admitted to transferring files between work and personal computers when working from home." [11]
>
> "18% of employees share passwords with co-workers. That rate jumps to 25% in China, India, and Italy." [11]

Those figures testify how relevant is the human factor as the big problem in cybersecurity. Surveys like this one carried out by the DSS Company [12] are very common and normally high lighten special product features. The aforementioned research reveals the existence of an environment that is dark and uncertain. Moreover, manufacturers often exaggerate with promises of highly efficient protection, sometimes beyond the scope of real security. Under certain circumstances, this assurance can hide threats, it´s to say, are misleading. Some faults are difficult to detect, such as enabling revoked users in crypto systems. Also, research institutes are attacked by hackers due to the nature of this activity.

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. [13] Recent publications about failures in many cryptographic application systems expose the level of access to private data. According to [14], [15] and [16] 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 to be revoked. For that purpose,, a wide range of cryptographic software has been tested, including TrueCrypt [17], VeraCrypt [18], GhostCrypt [19] and PGP Symantec Encryption Desktop [20]. All TrueCrypt deviants provide a unique password that grant user access to data. The problem, however, is that it doesn't matter how many times the user changes the password, for each one always open the container and expose the data.

When a trainee configures TrueCrypt or similar software for a business person, politician, high-ranking military or for a researcher, installing the piece of software with the password "123", the user is advised to change it to a "strong password". As this procedure is commonplace [21] [22] [23], billions of dollars' worth of data may be in the hands of the trainee. The way to gain access to the new data with the old password is to change the values in the reader of the container file. Similar problems have been identified by Symantec Encryption Desktop [16].

The typical Internet user enters his/her credentials many times a day. Logging into social media at the same time for maintenance purposes exposes their daily routine. The same is true when using an intranet and other web-based private systems in the workplace. 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 all common users are affected, the bulks gain global proportions. 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 which clients input important personal details), and on how these websites manage their users' passwords. Many different bank and retail websites have been tested and found to be vulnerable to password leakage.

As far as authentication problems are concerned, [24] it's worth consider three categories of attack. In the first one, known as *existential* forgery, an attacker can forge an authenticator for some unspecified user, which means that he/she cannot target one specific user. In the second, known as *selective* forgery, a specific user can be targeted. In the third and final category, known as *total break*, an attacker is able to recover the user key and can therefore build valid authenticators at his/her will.

In addition, [25] It´s also important to analyse a vast class of information about the navigation activities that browsers save onto the hard-disk. Credentials were found in the form of clear text in non-volatile memory. When the respective site failed to hide its login data, it's possible to extract the password. This occurred with all browsers tested by the author of the present paper, which means that, independently of the browser, Gmail, Amazon, eBay, Hotmail, and the Santander, Caixa and Citibank websites showed the same vulnerability [26].

Investigations into cryptographic programs, web browsers and web credentials have shown that the credential management, security and privacy protection measures are currently at a poor level. Meanwhile, investigations in to "in-private navigation" shows that the "privacy software" does not, in fact, gives the adequate privacy to the user. Many researchers have focused on the technologic aspects of those cases, such as flaws in the code written or project errors. Some studies the environment found in companies and governments, while others point out that the process can be corrupted. While all of them are correct in their conclusions, it is necessary to find the common factor in all these situations.

The technology already promises quantum cryptography; but, if vendors and users continue to manage credentials they are doing today, it will be like a locked car with the car key forgotten in its door lock. What can one expect from cybersecurity and privacy when our universities are encouraging the sharing of our 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." [23]

> "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." [21]

In the same way that universities orient their users towards using "in-private" navigation, one has to stand still and review what is being taught about security and privacy. [27] [28].

[29] Classifies cybersecurity according to 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 does 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." [5].

> "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 in security policy design." [5]

Agreeing with Sadok and Bednar, this author considers human-centricity as the best approach for address the cybersecurity problem. It´s necessary to adjust the whole background, specifically, the way cybersecurity and privacy are explained to the students and I.T. professionals.

Gal-Ezer et al. proposed five units to teach High School programming courses in Israel: fundamentals, advanced programming, second paradigm, applications and theory. Likewise, [30] declared 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 [31]. Unfortunately, no security or privacy aspects have been considered so far.

In New Zealand, there have also been discussions about Computer Science on the High School curriculum, without taking cybersecurity and privacy into account [32].

In the UK, researchers have been concerned with teaching Computer Science to produce more and more programming from the secondary level onwards [33] [34] [35].

> "The challenge of introducing security in a sensible and useful manner can be addressed by considering the contextual perspectives". [5]

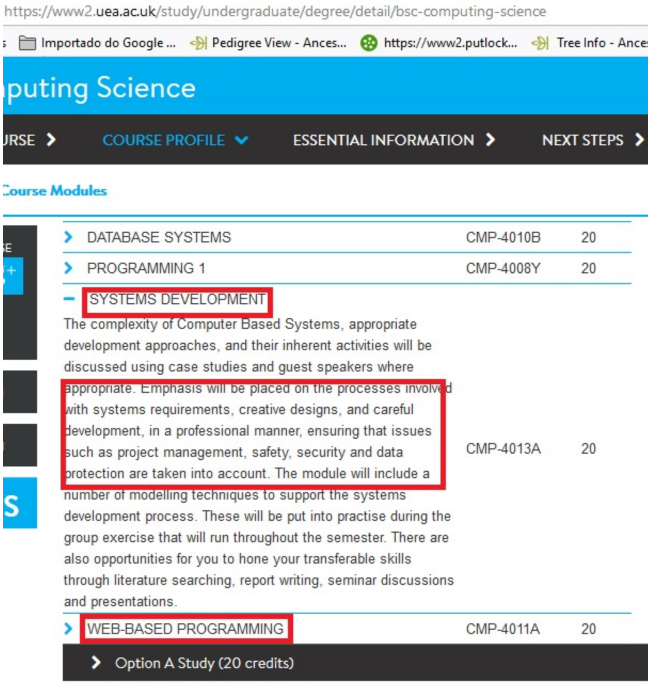
In this way, the basis of cybersecurity must be introduced in the early education, according to the Joint Task Force on Cybersecurity Education [36]. While this report provides guidelines for delivering cybersecurity education, all managers of technological courses could benefit from reading it.

III. METHOD AND DATA COLLECTION

From the perspective that everything has a human element, the author has gathered information to understand what UK universities are thinking about cybersecurity and how its people are being trained. For this, it is necessary to analyse the curricula of the offered courses. For that, one needs to study the common basis of those courses, disregarding cybersecurity specific courses. The intention here is not to evaluate cybersecurity as a specialist; but rather, to understand the impact rendered by the lack of study on security disciplines, in the context of Computer Science knowledge.

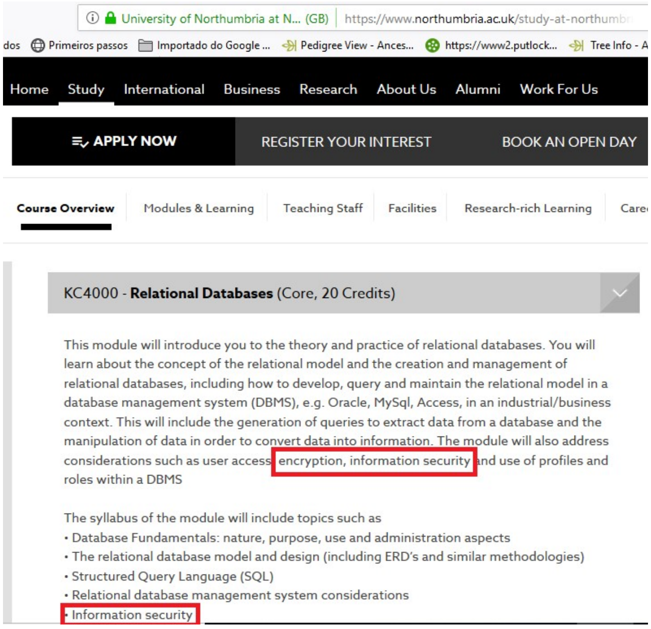
For this purpose, the author has considered the discipline components of 100 UK G400 Computer Science courses [37] or similar, from the top 100 UK universities offering such courses. The ranking used was the one prepared by the "Webometrics Ranking of World Universities", which is an initiative of the Cybermetrics Lab, a research group belonging to the *Consejo Superior de Investigaciones Científicas* (CSIC), the largest public research body in Spain [38]. This ranking includes 280 UK universities. This study considers that the first 100 UK universities represent a relevant sampling in the universe of UK universities in order to analyse the situation of cybersecurity disciplines on G400 courses in the UK. Computer Science courses focused in Cyber Security is discarded.

The title of the module or discipline and the content of the discipline as see on Fig.1, Fig.2 and Fig3., when available online, were manually read line by line to identify cybersecurity content keywords as security, privacy, cyber security, 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. The main focus was on identifying security elements for software development.



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.



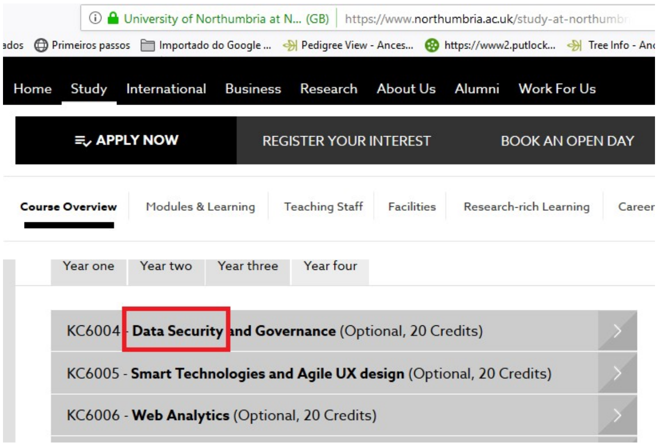
KC4000 - **Relational Databases** (Core, 20 Credits)

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, the totals are summarized in Table 1.

Annotations have been also made by the author also made to identify at which point in time the safety element was addressed, as well as whether the subject discipine was mandatory or optional.

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

Total of	Amount
courses	100
security content	189
optional security content	81
mandatory security content	108
courses without security content	13
courses without mandatory security content	39
security content in the year 1 of courses	32
security content in the year 2 of courses	43
Total security content in the year 3 or later of courses	114

IV. DISCUSSION

The absence of anything about security and privacy in the curricula says a lot about the relevance of this theme on the courses in question.

After the analysis of course grades, if the curriculum has one or more explicit citations about cybersecurity or privacy, a value of 1 was given, or 0, otherwise:

- 6% of security content in the UK G400 have no references to cybersecurity, privacy, secure programming or other cybersecurity content during the course, Fig. 4;
- 39% of G400 UK courses do not offer mandatory cybersecurity content, Fig 5;
- 17% of courses offer cybersecurity content in the first year of the course, Fog 6;

- 13 Computer Science Courses do not have any security content explicated in the curriculum Table 1;

For those analyses, It´s straightforward to notice that a total of 118 content areas identified in 100 Computer Science courses, some of those present more than one content area. Fig. 4 shows the proportion of mandatory cybersecurity content on Computer Science courses in the U.K, while Fig. 5 shows the proportion of any kind of cybersecurity content on these courses. Besides the importance of having security content included in the course curricula, it's necessary to analyse the disposition of this content across all the years of the course. This distribution is presented in Fig. 6. Our people learn to program without information on security issues.

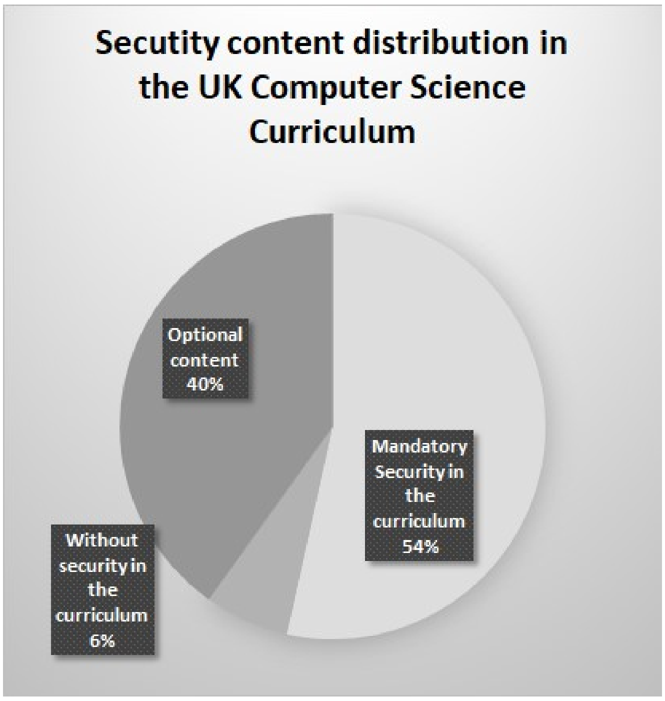


Fig. 4 Considering the total contents 118 under 100 Computer Science Courses, Security as a mandatory discipline or an element of other disciplines on UK computer science courses. 6% of courses have no security content on the curriculum and 54% of courses have mandatory cybersecurity elements on the curriculum and 40% have optional security content. Source: Table 1.

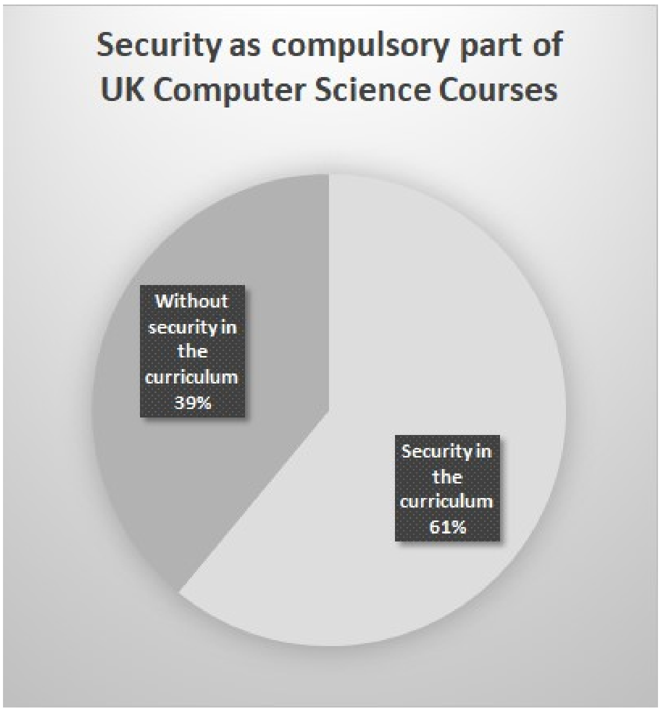


Fig. 5 Considering 100 Computer Science Courses, Security as an optional discipline or an element of others disciplines on UK computer science courses. 61% have security on the curriculum and 39% have no security on the curriculum. Source: Table 1.

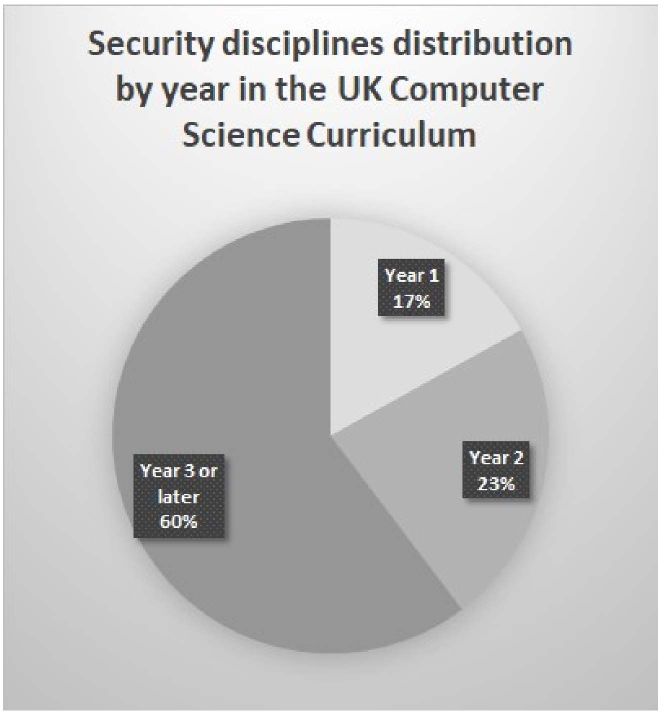


Fig. 6 Considering the total 118 security content, Security discipline's distribution by year on UK computer science courses. 17% focus on security content in the first year, 23% in the second year, 60% in the third year or later. Source: Table 1.

The data analysis indicates that more than one third of G400 courses in the U.K leave cybersecurity out of their mandatory curricula, while cybersecurity is an optional discipline, which is relegated to the end of the course in the case of the other two thirds.

According to the author of reference [6], people are at the centre of any technological design and for the author of reference [39], the education of cybersecurity content are failing to attend industry demands.

Forensic concept is not just a police issue. According to the author of reference [40], it is incorporated by the companies and that is time for Government and universities include its concepts into computer science courses taught.

One of principal challenges concerning digital privacy and security is the management of credentials. Credentials are literally “the key” and one need to encourage U.K users to keep safe the key. Meanwhile, developers need to design security systems without critical failures and breaches from the first line of code onwards. The existence and massive use of password-based authentication and their limitations and risk are explored by [41].

According to the National Academies Press, seven principles need to be observed concerning people learning and understanding of any subject/discipline. Some of those principles are highly relevant to this work:

Firstly, it is easier for students when they establish a firm foundation before adding new knowledge. All new knowledge is influenced by previous experience. 17% of exposition in cybersecurity concepts at the year 1 for Computer Science courses, including mandatory and optional content, is too little. When one learns how to cross a road, it is more difficult to adapt to the concept of a formal road crossing because the person always is influenced by his/her previous experience. Practising cybersecurity and privacy every day while on a Computer Science course will foster security mind-set, way of thinking and attitudes. [42]

To teach at the end of course and leave it optional is the biggest problem that this work likes to expose.

The first stage in the process of acquiring knowledge is to “remember” [43]. To remember something, one needs to be exposed to something new. In this work, it´s important to examine whether U.K students are being exposed to cybersecurity.

V. CONCLUSION

How then one can make cyberspace safer? It´s necessary to teach cybersecurity to Computer Science students since the very first year of school.

An ERP computer program or a website into which input the necessary credentials to get access to one’s bank account is normally developed with totally blind faith using the piece of software above mentioned. If an OS project fails, this is ignored by other actors because they know that the OS will save all data in the physical memory. The author is quite aware of browser developers who ignore the fact that false “in-private navigation” exists. One can have an SDK that offers a password field without any security requirements, if the preceding steps fail. Furthermore, this field can be dragged and dropped by the website developer.

The UK National Cyber Security Strategy 2016-2021 [44], in 7.1.1, states that directing efforts to invest in an increasing number cybersecurity specialists is misplaced, while quietly citing the precariousness of exposing cybernetic concepts to all computer-related courses only offers a thread of hope.

There is no point in continuing to create more and more courses for cybersecurity experts. Today, these professionals are involved in repairing programs with little notion of cybersecurity. At the same time, the vast majority of IT practitioners are not being properly trained to develop secure applications from the first line of code.

The world will have secure systems only when the first line of the first algorithm has been written under the mandatory cybersecurity premises, concepts and techniques. In the meantime, education and training are the more accessible ways to prevent and to fix cybersecurity problems.

Even with a large capacity of trained personnel pointed out in [45], a percentage that does not reach 10% of security content was offered until 2016 in the programs of Computer Science in the USA.

Cybercrimes are classified in seven categories according to [46], Phishing, Spam, Hacking, Cyber Harassment or Bullying; Identity Theft, Plastic Card Fraud and Internet Auction Fraud. To improve security in software development and increase difficult to cybercriminals, it’s necessary to reconfigure Computer Science courses. This work proposes a change in the teaching paradigm by including cybersecurity as a mandatory and explicit content throughout the duration of undergraduate Computer Science and software design courses and disciplines, so students will become proficient enough to develop secure pieces of software. Cybersecurity content must be formal and explicit in the programming disciplines.

Unfortunately, security requirements use to be considered just after the ‘conclusion’ of the design efforts of a given piece of software [47]; it’s to say, non-rarely seldom, after already being totally written.

As long as cybersecurity content is not written into the discipline’s syllabus, it is likely that it won’t not be taught at all the consequences of that being potentially disastrous, costing millions of pounds.

VI. REFERENCES

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

[2] H. E. S. A. HESA, “Higher Education Student Statistics: UK, 2016/17,” HESA, Promenade, 2018.

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

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

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

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

[11] Cisco, “Data Leakage Worldwide: Common Risksand Mistakes Employees Make.,” 24 02 2014. [Online]. Available: http://www. cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-pre vention/white paper c11-499060.html.

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

[13] A. &. S. M. A. &. L. T. V. V Barabanov, “Statistics of software vulnerability detection in certification testing,” *Journal of Physics: Conference Series.,* vol. 1015, no. 4, pp. 1-9, 2018.

[14] 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.

[15] R. Ruiz and R. Winter, “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.

[16] 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.

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

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

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

[20] 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].

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

[22] 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/.

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

[24] 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.

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

[26] 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.

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

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

[29] 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.

[30] 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.

[31] 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.

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

[33] 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.

[34] 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.

[35] 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.

[36] ACM; IEEE-CS; AIS SIGSEC; IFIP WG 11.8, "Cybersecurity Curricula 2017," ACM; IEEE-CS; AIS SIGSEC; IFIP WG 11.8, New York, 2017.

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

[38] Cybermetrics, "Webometrics," 2018. [Online]. Available: http://www.webometrics.info. [Accessed 04 02 2018].

[39] 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.

[40] H. Jahankhani and AminHosseinian-far, "Chapter 8 - Digital forensics education, training and awareness," in *Cyber Crime and Cyber Terrorism Investigator's Handbook*, B. Akhgar, A. Staniforth and F. Bosco, Eds., Elsevier Inc. , 2014, pp. 91-100.

[41] H.-F. A. Jahankhani H., "Challenges of Cloud Forensics," in *Enterprise Security. ES 2015. Lecture Notes in Computer Science*, R. M. W. R. W. G. Chang V., Ed., Springer, Cham, 2017, pp. 1-18.

[42] National Research Council, Division of Behavioral and Social Sciences and Education, Board on Testing and Assessment, "Learning with Understanding: Seven Principles," in *Learning and Understanding: Improving Advanced Study of Mathematics and Science in U.S. High Schools*, Washington, DC, National Academies Press, 2002, pp. 117-130.

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

[44] UK Government, "National Cyber Security Strategy 2016-2021," 2016. [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf. [Accessed 15 January 2018].

[45] S. C. Y. &. B. Wen, "Toward a cybersecurity curriculum model for undergraduate business schools: A survey of AACSB-accredited institutions in the United States," *Journal of Education for Business,* vol. 92, no. 1, pp. 1-8, 2017.

[46] H. Jahankhani, AmeerAl-Nemrat and AminHosseinian-Far, "Chapter 12 - Cybercrime classification and characteristics," in *Cyber Crime and Cyber Terrorism Investigator's Handbook*, Elsevier, 2014, pp. 149-164.

[47] R. M. S. C. Hosseinian-Far A., "Emerging Trends in Cloud Computing, Big Data, Fog Computing, IoT and Smart Living," in *Technology for Smart Futures*, A. H. A. B. Dastbaz M., Ed., Springer, Cham, 2017, pp. 29-40.