The Challenges of Integrating Industry 4.0 in Cyber Security — A Perspective

Yvonne James and Olivier Szymanezyk

***Abstract*—We adopt Industry 4.0 (I4.0) and professional qualifications for adapting models of deliveries of teaching the module of Cyber Security at the University of Lincoln (UK). To achieve this, we investigate I4.0, the challenges it sets to higher education, and professional qualifications. Our findings are used to devise three models of delivery, namely Comprehensive, Partial and Merged. Our discussions show that our strategy of the integration of I4.0 within the curriculum development effectively prepares students to stand out from the crowd by possessing industry ready accreditations along their computer science degrees and the skills required for their future career in cyber security.**

***Index Terms*—Assessment strategy, curriculum development, cyber-security, industry 4.0.**

I. Introduction

The University of Lincoln (UoL) was inaugurated in 1996 by Her Majesty the Queen to respond to the demand of local educational requirements of Lincolnshire (UK). Throughout its twenty years of existence, over £170 million has been invested in UoL to transform a brownfield site into an award-winning, state-of-the-art learning, teaching and research environment. In 2019, UoL has over 14,000 students and 1500 staff members. It provides an educational experience based on core scientific disciplines, conducts world-leading research in its areas of focus, and maintains and expands partnerships and links with regional, national and international bodies from both industry and academia. In recent years the university has been awarded the Gold standard for the Excellent Teaching Framework (TEF). 95% of students find employment within six months of completing their chosen programme of study, making it an increasingly popular choice for home and international students. UoL ranks overall fifth in the regional East Midlands university table and has risen to the 43rd in the UK-wide league tables [1].

The engagement with external non-academic and industry partners is a crucial element of UoL's long-term strategic plan. It answers to regional economic needs by co-operating with local businesses and employers, e.g. the National Centre for Food Manufacturing (NCFM) and Siemens. This engagement is consistently appreciated by the current, and future business need. It ensures progression opportunities at every level of achievement while providing a smooth transition between the different environments of universities and business [2]. External industrial partners such as Siemens, Microsoft and Cisco are encouraged to be involved with the design, revalidation and delivery of UoL's educational program to achieve these changes.

However, modern society and economy are experiencing profound transformations which result in a global transition and convergence of disciplines within higher education, academia, and industry. These contemporary societal and economic developments are stimulated through the rapid advances in technology, which drove the emergence of a phenomenon known as Industry 4.0 (I4.0) [3]. I4.0 is the result of a Germany-based initiative which aims to strengthen the economy and to support the promotion of full computerisation of every level of manufacturing [4]. This latter concept has been extended to accommodate computerisation of additional relevant industry sectors. Ultimately, I4.0 strives to embrace every aspect of the industry. These require the workforce of the future to be prepared and adequately trained to meet the needs of the industry.

Cyber Security is a module available to undergraduate students at the School of Computer Science (SoCS). It teaches students to critically evaluate the security of a computer system, to differentiate between types of cyber-attacks and critically assess their impact and to examine suitable strategies, policies and approaches to mitigation in light of legal, social, ethical and professional issues. However, with the development of I4.0, cybersecurity is facing unique challenges due to threats of cyber-crime due to the use of information technologies emerging through the concept of I4.0. For instance, the widespread use of the Internet of Things (IoT) leads to an increase in the number of interconnected companies, which automatically result in a severe evolution of a potential cyber attack target. Due to the challenges presented by I4.0, we recognise the necessity for programme changes through revalidation.

We aim to advance the teaching with a focus on a Cyber Security module within the context of higher education and I4.0. We adopt the benefits of embedding professional industry-recognised qualifications of the industry within higher education. Our main contribution is three models of delivery that offer opportunities to develop workshop and materials to embrace the challenges set by I4.0 within the curriculum. We discuss that our approach effectively forms win-win loop scenarios for graduates to obtain renown qualifications and vital technical skills in cyber security alongside their Computer Science degree to encourage graduates. They obtain a sturdy foundation, helping to prepare for their future career uniquely.

We first discuss previous work in I4.0 and the challenges

Manuscript received March 29, 2020; revised January 28, 2021.

Yvonne James and Olivier Szymanezyk are with the University of Lincoln, Brayford Pool, Lincoln, LN6 7TS, United Kingdom (e-mail: YJames@lincoln.ac.uk, OSzymanezyk@lincoln.ac.uk).

doi: 10.18178/ijiet.2021.11.5.1518

that it sets for Higher Education with a focus on teaching Cyber Security. Then we present our computer science curriculum at UoL, and we detail how the Cyber Security fits within it. We then discuss Professional Qualifications, and they prepare students for I4.0. Lastly, we present our three models of delivery, and we discuss our experiences and perspectives of our approach.

II. Industry 4.0

Industry 4.0 (I4.0) is the culmination of a German-led initiative to develop the economy and promote the computerisation of manufacturing [4]. This notion has been extended to provide computerisation of every industry sector. For instance, manufacturing comparing are taking a great interest in I4.0 as it provides them to operational efficiency, productivity and customisation features. It provides the industry solutions to deal with huge data volumes, developing human-machine interactive systems and improving communication between the digital and physical environments [5]. Ultimately I4.0 will encompass every aspect of the industry. Bonner [6] identifies four principles which are determined to lay out the foundations of I4.0:

- *Interconnection*: The ability for people to connect and communicate through devices via the Internet of Things (IoT) or Internet of People (IoP).
- *Information transparency*: The ability to collect and process vast amounts of data to reach meaningful information, leading to improved decision making, improvements and innovation.
- *Technical assistance:* The ability of cyber-physical systems to support human activity by undertaking a range of tasks that are unsafe for humans or conducted in difficult environments.
- *Decentralised decisions:* The field of autonomy where cyber-physical systems are designed and build to have autonomous decision-making capabilities.

Industry 4.0 has been the catalyst for growth in the manufacturing sector having been seen as a successful mechanism to improve efficiency, productivity and push towards a higher level of automation.

III. Challenges in Higher Education

I4.0 presents a massive challenge to prepare the workforce of the future if there is to be any chance of success. [4]. Consequently, it represents significant challenges to Higher Education (HE) to meet the four principles and ensure that graduates are armed with a raft of technical skills as well as their academic development.

We recognise I4.0 as an opportunity to engage with academic and industry partners to revalidate the computer science curriculum. This will effectively allow changes to modules to enable the principles to drive a move towards skills development that fulfils I4.0. Given this context, I4.0 has been identified by UoL as content applicable to AI and Robotics, Cyber-Physical Systems, Machine Learning and Big Data as identified in Fig. 1. There are links between manufacturing and computerisation, which then feed into the four pillars of I4.0.

We contend that there are two approaches to address the challenges set by the integration of I4.0:

1) Deliver modules with learning objectives specifically tailored to the four principles of I4.0.
2) Include professional qualifications in undergraduate and postgraduate modules that have been developed by industry-leading experts.

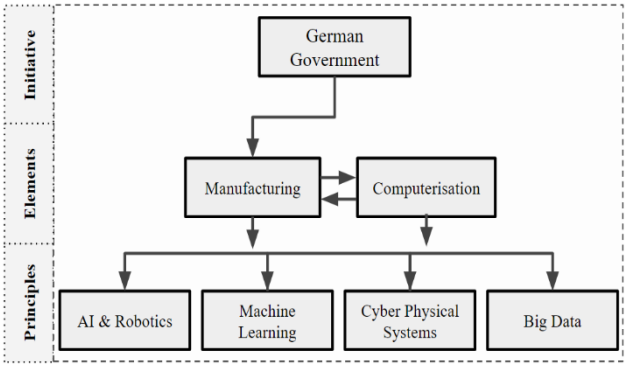


Fig. 1. Applications of I4.0 in higher education.

However, the application of these approaches is not straightforward. For instance, higher educational institutions may need to employ staff with relevant technical capabilities as well as academic knowledge. In our experience, this always been the case in Further Education FE colleges, but less so in universities given that study is academic and therefore research focused as opposed to the vocational study undertaken in the FE sector [7].

Nevertheless, the application of these approaches is not straightforward. For instance, higher educational institutions may need to employ staff with relevant technical capabilities as well as academic knowledge. In our experience, this always been the case in Further Education FE colleges, but less so in universities given that study is academic and therefore research focused as opposed to the vocational study undertaken in the FE sector.

Additionally, there is also a recognition that the UK Government has challenged secondary education to deliver computer science-related curriculum. The knock-on effect of this change is that students in the next 5 to 10 years will arrive at university with a high-level of programming skills. In response to this challenge, UoL is reviewing the curriculum to provide students with the academic challenges they expect.

Nevertheless, both approaches ensure that students are equipped with high-level technical skills. By contrast, computer science students at UoL have a breadth of knowledge which equips them to be able to apply for a much broader range of graduate opportunities. In one respect these two contrasting approaches both meet the needs of industry, but in another sense, only the former addresses the technical skills required of I4.0. The challenge to HE is how to achieve a better balance which provides the same level of academic development but also addresses I4.0 without losing sight of academic standards and subject benchmarks.

IV. The Rise of Cyber Security

The teaching of cyber security has gained in importance

across providers in the UK at all levels. The number of higher education providers that are offering Cyber Security as part of their curriculum for the academic year 2019/2020 as a subject choice or part of a degree programme has increased significantly. Table I indicates undergraduate cyber security courses available for the academic year 2019/20. The figures represent all HE providers offering cyber security courses and provide a comparison from the offering in 2018/19 and 2019/20. The most significant increase is in England where 25 additional providers include cyber security in their academic offering. It demonstrates a 56% change in courses with a 63% change in providers. An increase in providers of 52% and 53% for courses, underpins the importance of cyber security for HE in the UK. This level of increase indicates that other HE providers are also likely to follow suit.

TABLE I: UNDERGRADUATE CYBER SECURITY DEGREES THROUGHOUT THE UNITED KINGDOM

	2018/19		2019/20	
Location	**Courses**	**Providers**	**Courses**	**Providers**
England	34	18	78	48
Wales	5	2	8	3
Scotland	4	3	6	4
UK	43	23	92	48

V. CYBER SECURITY AT THE UNIVERSITY OF LINCOLN

In 2017, the School Of Computer Science confirmed a new Cyber Security module. It teaches students the security of networked computer systems, shows different types of cyber-attacks, defence strategies, policies and approaches of damage mitigation, including discussions about ethical and legal issues. The module was developed to take the full advantages of using different virtual environments (VM). They provide a toolset of penetration testing tools and attack platforms. In addition, on-site servers running different operating systems can provide further points of attack platforms. Students are able to probe a multitude of operating systems to discover vulnerabilities using penetration testing tools. The VMs consists of different versions of Ubuntu Linux, Windows 2000 and 7. Ports can be were opened on purpose allowing students to experiment with various attack tools. Files containing specific information were created, as were users. This helped them understand how attacks were carried out from the reconnaissance phase through to gaining access and finding data. Students are assessed through a series of in-class tests and assignments which include the investigation of existing online network security breaches.

An experienced lecturer with an industry background was appointed to deliver this new module for 2017/2018. During the first run of the Cyber Security module, there were some unexpected complications. The first of these related to the make-up of the cohort. They included those who had a technical (e.g. experience in programming or games development, etc.) and theoretical background (e.g. social computing, information systems, etc.) in computer science. While students with a theoretical background were small in number, they provided a challenge of delivering the intrinsically technical module of Cyber Security to non-technical students. A further challenge was to develop workshop activities that successfully strengthened the lectures' content whilst being appropriate for the cohort's skill. The workshops were primarily designed for more technically-apt students, but they have had to include a varied level of difficulty. This was primarily due to offer options to the non-technical cohort to accomplish the tasks whilst permitting them to develop relevant skills and knowledge. In 2018/2019 the delivery of Cyber Security, the cohort consisted of only computer science students allowing for the workshop sessions to become more technical. For example, students were able to explore cryptographic processes in more detail and used software to simulate network intrusions and detection. The assessment allowed for more technical aspects to be covered which assessed the students' knowledge and technical understanding. The use of an in-class test presents an opportunity to provide an alternative type of assessment which explores the practical skills learned throughout the workshop sessions. Furthermore, throughout that year, we encouraged a handful of students to participate in a series of pilot schemes to explore possible models of delivery of the Cyber Security content.

However, after two years of delivering Cyber Security, it was acknowledged that the module had to undergo abundant changes to its curriculum. We considered it as an opportunity to invigorate the module in line with I4.0, and to explore new methods of delivery. Furthermore, we investigated the importance of industry professional qualifications and we decided to include them as part of the curriculum.

A. Changes to the Curriculum

In 2019, the SoCS proposed changes to the whole computer science curriculum to reflect the I4.0 initiative in higher education. In respect to this, the new curriculum aims to addresses the challenges of I4.0.

In the first instance, programming modules are enhanced to extend the number of languages taught, with Python becoming a major component in the first year. As students' progress through the second and third years of study, they are introduced to modules including Machine Learning, Cyber Security, IoT, Data Analytics, all of which meet with the four principles as indicated by Bonner [6]. To bolster this further, and in support of the I4.0 initiative, professional qualifications are offered alongside degree programmes.

B. Professional Qualifications

Employers look for the development of soft skills, high-level technical skills and professional qualifications. Students can develop their soft skills through part-time work while at university and technical skills are developed throughout the degree programme. The professional qualifications present a different challenge as they contribute towards readying graduates to become even more work ready. For UoL this has meant the introduction of the Cisco Certified Network Associate (CCNA).

The CCNA offers industry standard certifications from Cisco Systems [8]. It is renowned for high quality, demanding computer networking courses leading to professional qualifications which are very attractive to employers. As this is a single standalone course, students do not need to complete the full CCNA to have the right level of understanding. The Cyber Operations course covers the

required elements. There is an extensive range of lab exercises so students can very quickly understand the make-up and functionality of networks in the first instance. It is furthermore enhanced by the use of a virtual environment composing of:

- Cyber ops Workstation, containing several preset events which students interact with to identify threats and vulnerabilities
- Kali Linux, which contains a wide range of tools for penetration testing.
- Security Onion, which is an industry standard application containing tools for tracing attacks
- Metaspoitable, which provides an attack platform. [8]

VI. Models of Delivery

We intend to embed professional industry-recognised qualifications within the curriculum. To achieve this, we developed three models of deliveries which are detailed below:

- CMD: Comprehensive Model of Delivery
- PMD: Partial Model of Delivery
- MMD: Merged Model of Delivery

A. CMD: Comprehensive Model of Delivery

In this model, the modules use materials developed by the awarding body. In the case of UoL, this would be the Cisco Systems Plc. The module is made up of the relevant presentations and workshops. Cisco provides 12 presentations and accompanying workshops. [8] Students can undertake preparatory reading by using the online curriculum and a combination of physical devices and simulation software to replicate the real-world environment for workshops.

Online assessments are integrated into the provider's assessment strategy. There are some concerns with this as the examinations set by the awarding body are multiple choice questions (MCQ). This method of testing is not always seen as robust for undergraduate study, and is often referred to as "multiple guesses". While students are expected to complete the chapter exams, final exam and skill-based practical test, there is also scope for instructors to include additional assessments which may be seen as bolstering the university assessment strategy. The full model allows for the professional qualification to be studied and gained in full.

Consequently, the study and qualification are tied directly into the curriculum. In some instances, students have to pass one part of the qualification to proceed to the next part. For example, passing CCNA semester 1 to proceed to CCNA semester 2. In other cases, the qualification may stand alone – Cisco Cyber Operations (CCO), for example [8].

B. PMD: Partial Model of Delivery

In this model, students are still able to undertake preparatory reading and use the simulation software for the workshop materials. Examinations can be done away from the university in less formal settings with the final exam and skill-based practical being conducted under exam conditions. There is some teaching as required. This is often at the request of the students for areas of the curriculum they might be struggling to understand.

C. MMD: Merged Model of Delivery

This model allows professional qualifications to be studied independently by students, without the need to host formal lectures. This choice is left to the provider although pre-recorded or live streamed lectures provide alternatives.

The latter does give the students an added advantage of being able to watch a lecture in their own time. There may be an element of discussion between lecturer and student to explain difficult technical content. Workshops can be done either in the university's networking lab using the specialist equipment or simulation software. For some subject areas' students are expected to gain experience through hands-on exposure to equipment. Providers often offer summer or weekend schools which students attend in person.

VII. Discussions

The Cisco curriculum is broken down into various assessable elements. There is a considerable amount of reading, supported by tutor-led teaching and enhanced by a wide range of challenging but interesting labs. The combination of physical equipment and simulation software means that students can gain significant skills and knowledge in computer networking. This makes them very attractive prospects in the employment market.

However, not all providers have either the staff or the capability to deliver professional qualifications so many degrees are still delivered in the traditional manner. For those universities who do have the capability, the additional professional qualifications provide a number of economic and academic benefits to students as underlined by DiCerbo [9]. Many institutions have created a specialist degree that allows for the integration of the CCNA. Essentially, the four semesters, as defined by Cisco [8], [9], become four modules in the degree programme. The inclusion of these modules provides an excellent opportunity for students to become Cisco CCNA qualified. To provide more context here, each semester has in the region of 11 chapter exams and a final exam, all of which are multiple choice questions. These can have a weighting applied which can have a bearing on the overall grade for each semester. In addition, there is a hands-on skills exam that tests the practical application of the skills learned. There is also a facility which allows Cisco instructors to create their own assessments. Furthermore, in the job market graduates have a competitive advantage over others by being able to add a professional qualification to their CV. The figures presented in Table I above also contain cyber security, forensic computing and information technology, all of which contain modules on computer networking. This means that there are not 71 providers all offering professional qualifications and therefore the choice of provider is somewhat less. The provider also has the choice of which model of delivery they opt for given the nature and number of students.

Pilots were run in 2018/2019 to investigate our models of delivery. Although this was met with initial trepidation, schemes have encouraged a handful of students to participate. Discussions with the students during and after the course

have proved to be very encouraging. Students have enjoyed the practical hands-on nature and the exposure to technologies over and above the degree module content. There is a considerable amount of self-study involved and students have enjoyed being able to work at their own pace while knowing they still have access to lecturer support when they need it in addition to the taught sessions. There is also complete flexibility in the assessment process, allowing students to take topic tests whenever they are ready and not to a prescribed time. Over 20 final year students have registered. At the time of writing this paper, only 3 have successfully completed. The remainder of the group will continue after exams have finished enabling then to concentrate on degree assignments first but then wholly on the Cisco Cyber Operations course before the holiday period.

Nevertheless, the initial uptake for Cisco courses has seen around 30 students register. The volume of work involved was considered as daunting and many students had never come across this type of study. There are two other aspects to take into consideration. Firstly, the newly created Cisco Network Academy did not initially have any physical equipment that students should be exposed to. Secondly, this is a long-term initiative, concentrating more on the delivery of the Cyber Operations course which is a single semester and addresses both the skills gap and I4.0. Ultimately some of the Cisco provision could be validated within an MSc programme.

Conclusively, the comprehensive model of delivery has been chosen as the preferred method of delivery for delivering Cyber Security for 2019/2020. Students are taught in a structured format, working with the detailed curriculum week-to-week. This provides full integration with the degree curriculum. This means that the professional qualification is an integral part, validated and credit earning. The mix can meet the demands of I4.0 by including courses that cover security, database, programming and cloud. The CCO Operations covers the cybersecurity element. Cisco also offers a range of free short courses to introduce IoT, Python, Network Programming and Linux to encourage engagement with other more technically demanding qualifications.

VIII. Conclusion

The engagement with external non-academic and industry partners for them to be involved with the design, revalidation and delivery of UoL's educational program is a key element of its strategic plan. However, due to the use of information technologies emerging through the concept of I4.0, cyber security is facing unique challenges that the workforce of the future has to be prepared for. There are still gaps to fill in higher education as I4.0 is heralded as an initiative for the next industrial revolution. There are challenges around the further development of undergraduate curriculums and the continued offering, which can be addressed with the integration of professional qualifications.

Throughout this paper, we are presenting our perspectives on integrating the challenges set by I4.0 in Cyber Security module. We report on the results of the observations and pilot studies from delivering the module between the academic years of 2017 and 2019. We discuss how professional industry-recognised qualifications are embedded within the curriculum, and we developed three models of deliveries, namely the Comprehensive Model of Delivery. Partial Model of Delivery and Merged Model of Delivery. Our initial results show that our approach was initially found as daunting by students due to the amount of extra work, but they appreciated working on their own leisure on extra qualifications. The Cyber Operations course provides a high level of understanding about attacks, how to mitigate threats and introduces an interesting toolset to the cyber analyst of the future. We will continue to expand the Cisco Networking Academy to allow first and second-year students to participate, enhancing their skills and knowledge and boosting their future employability. This is the first step towards making curriculum changes in light of I4.0. As part of the revalidation process, the four pillars of I4.0 are addressed through the inclusion of new modules. Furthermore, considering that this is the first offering of course to the computer scientists of the future, who is interested vary and are not specific to computer networking, this initial uptake is promising. Cyber Security continues to be a growth area and is attracting interest from many areas of computer science.

However, this is the first stage of our work. We intend in future work to explore different engagements of additional I4.0 integration within Higher Education and work towards our next step to integrate industry standard professional qualifications within the Cyber Security module. Furthermore, future work should address running models of pilot studies of different models of delivery within a variety of I4.0 related modules, which would allow us to obtain further data to reflect on our continuous engagement of I.40 within Higher Education.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Olivier Szymanezyk conducted research into the academic landscape. Yvonne James conducted research into the course offerings and produced the data analysis. The paper was written jointly. All authors approved the final version.

Acknowledgement

We would like to thank Dr. Derek Foster, who has supported and encouraged the inclusion of professional qualifications in his role as Programme Leader at UoL. Dr. Kevin Jacques, who inspired the collaboration on this paper.

References

[1] The Complete University Guide Independent Ranking 2019. [Online]. Available: https://www.thecompleteuniversityguide.co.uk

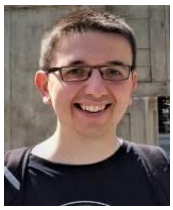
[2] D. Charles, R. Ahoba-Sam, and M. Salomaa, "On overcoming the barriers to regional engagement: Reflections from the University of Lincoln," *RUNIN Working Paper Series*, vol. 2018, no. 4, 2018.

[3] M. Munsamy and A. Telukdarie, "Application of industry 4.0 towards achieving business sustainability," in *Proc. IEEE International Conference on Industrial Engineering and Engineering Management*, 2018, pp. 844-848.

[4] Y. Lu, "Industry 4.0: A survey on technologies, applications and open research issues," *Journal of Industrial Information Integration*, vol. 6, pp. 1-10, 2017.

[5] B. C. Ervural, "Overview of cyber security in the industry 4.0 era," *Industry 4.0: Managing the Digital Transformation. Springer Series in Advanced Manufacturing*, Springer, Cham, 2018.
[6] M. Bonner. What is industry 4.0 and what does it mean for my manufacturing? [Online]. Available: https://blog.viscosity.com/blog/what-is-industry-4.0-and-what-does-it-mean-for-my-manufacturing
[7] M. Gusev, S. Ristov, and A. Donevski, "Integrating practical CISCO CCNA courses in the computer networks' curriculum," in *Proc. IEEE Global Engineering Education Conference*, 2014, pp. 499-506.
[8] Cisco. (2019). Be a cyber defender with cybersecurity courses | Networking academy. [Online]. Available: https://www.netacad.com/courses/security
[9] K. E. DiCerbo, "Hands-on instruction in the cisco networking academy," in *Proc. Fifth International Conference on Networking and Services, Networking and Services*, 2009, pp. 581-586.

Yvonne James is a senior lecturer in computer science (cyber security) in the College of Science. She joined the University of Lincoln in 2017 and currently teaches on two modules: Network fundamentals and cyber security. Yvonne has been involved with the management of high performance computing infrastructure. She has been the research assistant for an innovate UK project on energy efficiency in data centres. Her specialist interests are in the development of adaptive routing mechanisms for computer networks, software defined networking (SDN), cyber security including blockchain and malicious packet identification. She also has a keen interest in delivering industry certifications to support curriculum and provide students with valuable qualifications to enhance their employment opportunities.



Olivier Szymanezyk is a lecturer in computer science (games computing) at the University of Lincoln (UK). His role involves the organisation and management of the delivery of university modules about games development, programming, coding algorithms and paradigms, software design and games design to undergraduate and postgraduate students. Olivier's research background extends to agent-based modelling to improve the believability of large-scale virtual world environments. His work has contributed to publications in the advances in digital games research, playful experiences, multi-agent applications, the study of artificial intelligence, computational collective intelligence research, the simulation of pedestrian dynamics and to indoor navigation and routeing systems.