English, R., & Maguire, J. (2023). Exploring student perceptions and expectations of cyber security.
In CEP '23: Proceedings of the 7th Conference on Computing Education Practice (pp. 25-28). (ACM International Conference Proceeding Series).
Association for Computing Machinery.
https://doi.org/10.1145/3573260.3573267

Exploring Student Perceptions and Expectations of Cyber Security

Rosanne English
University of Strathclyde
Glasgow, Scotland, United Kingdom
rosanne.english@strath.ac.uk

Joseph Maguire
School of Computing Science
University of Glasgow
Glasgow, Scotland, United Kingdom
joseph.maguire@glasgow.ac.uk

ABSTRACT

Designing cyber security modules in Higher Education can be a balancing act. We aim to ensure students develop an understanding of key cyber security concepts such that they are able to contribute to security practices within the workplace. We also aim to develop understanding of more advanced and theoretical aspects of cyber security to meet a range of accreditation requirements and ensure those who wish to go on to work in security are suitably prepared. Additionally, students often have existing expectations and perceptions which must be managed. However, many general computing science degrees address security in isolated modules. As a result addressing these requirements can be challenging in the timeframe available. In this paper we present an activity designed explore student expectations of cyber security classes at two UK Universities in order to highlight the concerns of students such that curricula can consequently be amended to better meet student expectations.

CCS CONCEPTS

• **Applied computing** → **Education**.

ACM Reference Format:
Rosanne English and Joseph Maguire. 2023. Exploring Student Perceptions and Expectations of Cyber Security. In *Computing Education Practice (CEP '23), January 6, 2023, Durham, United Kingdom.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3573260.3573267

1 INTRODUCTION

Cyber security is a key element of computing science focused degrees. This importance is reflected in the requirements for accreditation such as the British Computer Society degree programme accreditation [1]. Cyber security is also critical component of subject benchmarks such as the QAA Computing Benchmark Statement [5] . In addition to recognition in the computing science higher education landscape, cyber security continues to gain more focus in industry and government. By 2025 it is predicted there will be 3.5 million cyber security job openings [13]. In attempts to address this skills gap, the U.K. government have tried to engage young people in cyber security through initiatives such as CyberInvest [11]. CyberInvest provided a range of routes into degrees. However, these initiatives have not claimed success in attracting students to the field. As such, we must look to generalist computing degrees to ensure we engage students in developing critical cyber security knowledge and skills.

In developing programmes and modules to meet this demand, we must balance a range of sometimes conflicting goals. One goal is covering key elements required by accreditation and addressed in curriculum benchmarks, ensuring students who wish to follow a cyber security career path have sufficiently advanced knowledge and understanding so as to allow them to obtain jobs in the field. However, we must also recognise that whilst many students will not move into a security focused role, they will play an important role in maintaining security in the organisations they work for. Additionally, there is also a need to manage student expectations which can range as wide as the field of cyber security itself.

Given the tendency for generalist programmes in the UK addressing cyber security in a single module [3], achieving these goals can be challenging. In an effort to better understand student perceptions and expectations of a cyber security module, in this paper we present an activity which gathers student perceptions and expectations in order to better manage student expectations alongside the other goals identified above.

2 BACKGROUND

Across the world there is increase in cyber security incidents [9]. Governments are responding to this increase in attacks by making cyber security a priority area. For example, in the U.K. we have a National Cyber Security Strategy 2016-2021 [7]. To succeed in such strategies we must examine whether we have sufficient skills and capacity. Both government and industry believe there is a cyber security skills gap [8]. By 2025 Cyber Security Ventures predicts there will be 3.5 million cyber security job openings [13].

One approach to addressing the cyber security skills gap is through education. This is a priority for the U.K. government, and has resulted in the National Cyber Security Skills Strategy. This strategy places a focus on funding digital courses on cyber security for everyone, no matter their background, age, or ability [6]. Whilst it is clear there is demand for security courses, it is less clear what students expect from such a module. Many conflate the terms computer security, information security and cyber security [14]. The topic varies widely and covers a range of roles such as Information Security Officer and Penetration Tester amongst many others.

Students entering Computing Science related degrees are often aware of cyber security and express interest in seeing it included in the curriculum. For example Kinnunen et al. explored student expectations upon starting a computing science focused degree across three institutions. A total of 345 students were surveyed about the expectations of content amongst other aspects. Without prompting on security specifically, the authors noted that computer

CEP '23, January 6, 2023, Durham, United Kingdom

ACM ISBN 978-1-4503-9821-3/23/01…$15.00
https://doi.org/10.1145/3573260.3573267

systems (including security) was identified 79 times [10]. Kinnunen et al. note that students appear to engage with higher education with specific topics in mind, one of which being cyber security [10].

Students often have expectations of what topics they believe such a module should cover. When these expectations are not met, students can become disengaged. This perspective can change post-graduation once students experience working in industry for a time. For example, Dziallas and Fincher interviewed two individuals who completed their degree in a computing science, and have now worked in industry, about their expectations of the curriculum and how it has changed [4]. One former student notes they are a "less harsh critic of the curriculum" [4]. Similar work has been completed by Begel and Simon [2].

This balance of requirements and expectations from students and industry can be a challenge. In this paper we present an activity designed explore student expectations of cyber security classes at two UK Universities in order to highlight the concerns of students such that curricula can consequently be amended to better meet student expectations.

3 ACTIVITY CONTEXT AND STRUCTURE

To establish student expectations for cyber security modules a survey was designed using a structure similar to Ogle's K-W-L teaching model [12]. This teaching model asks students to identify what they know, what they want to know, and what they have learned. This provided scope to identify any existing experience, both professional and otherwise, as well as what students wanted to learn from the module and a reflective element examining how they saw its contribution to their future career. To address these elements, the survey asked the following questions.

(1) Do you have any relevant professional computer security experience? If Yes, what is your experience. If no, why not?
(2) What have you already learned about computer security and from what venue?
(3) What do you want to learn about computer security?
(4) What skills do you consider important for a professional in computer security?
(5) How do you perceive computer security knowledge contributing to your future professional role?

This survey was presented to students at the start of delivery of two cyber security modules. The modules were run at two U.K. based institutions. Students were informed the survey was entirely optional and anonymous.

The first module is 'Computer Security' which covers the fundamentals of systems security and is a required class taught to 4th year undergraduate honours students. It is run for students on Computer Science, Software Engineering, Computer and Electronic Systems, and Mathematics and Computer Science degree programmes. It is a required module for Computer Science and Software Engineering students, and optional for the remaining degree programmes. Around 10% of students have experience in industry through a one year or summer placement. At the time of delivering this activity, Computer Security had 125 students enrolled. This module is the only security module, and as such is the primary mechanism for covering BCS Accreditation requirements related to security [1].

Theme- Have you had cyber experience?	ECS (M)	CS (BSc)
No	21 (60%)	48 (53%)
No, I haven't had an opportunity	0 (0%)	18 (20%)
No, but I would like to	1 (3%)	2 (2%)
No, I have no interest	0 (0%)	3 (3%)
Yes	13 (37%)	17 (19%)
Not answered	0 (0%)	3 (3%)

Table 1: Cyber Security experience responses

The structure of Computer Security is that of a flipped classroom. Students are asked to watch videos, complete reading and practical exercises related to the material for a given week before attending class. Contact time includes two in-person sessions per week which explore topics in more depth through tutorials.

The second module is 'Enterprise Cyber Security' and addresses a more business focused view of cyber security. It is taken predominantly by Masters students who are required to take the module. The Masters cohort are students who have an undergraduate degree in a field different to computing science. This is sometimes referred to as a 'conversion' programme. Enterprise Cyber Security is also taken by 4th year students who can take it as an optional class. At the time of running the exercise, this module had 212 students enrolled. This module does not contribute to BCS accreditation. The structure of Enterprise Cyber Security is two classes in a week. It follows an active learning approach in which students are presented with material in short lecture form interspersed with interactive activities such as think-pair-share and class wide discussions.

4 RESULTS

There were 91 responses (around 73% of the class) from the Computer Security class and 35 responses (around 16%) from Enterprise Cyber Security. Responses for each question were analysed to identify common themes. Each question will be discussed in turn.

4.1 Relevant Prior Work Experience and Knowledge

Answers to whether students had prior work experience relevant to cyber security resulted in five themes. A count for each of the answer themes is provided in 1 which shows the split between each response theme for both the Computer Security 4th year module, and the Enterprise Cyber Security Masters module.

Students who answered yes for prior experience in the Computer Security module often related experience in a software development role. This was generally through internships where students had been asked to examine a particular aspect related to security. For example participant 4 identified as having been responsible for exploring approaches to authentication within the company they worked for.

For Enterprise Cyber Security those who answered yes were more focused on business aspects of security. For example participant 8 said they were involved in "adhering to software policies and organisational GDPR policies". The contrast of technical vs.

non-technical here is not surprising as this cohort of Masters students typically have little or no computing background, and often have more business experience than undergraduates.

Only students from Computer Security identified as not having had an opportunity to engage with computer security. This is likely due to the cohort predominantly being students completing their first degree after leaving school.

Overall the responses to this question were generally as expected. Most students reported little or no industry experience in cyber security. However, it was surprising that so few students identified as having an interest in cyber security. A total of 5% of student responses indicated a desire for developing cyber knowledge and skills. This information could be used to tailor delivery of a module to a given cohort, those with less interest could benefit from more focus on how security impacts a wider scope of jobs and personal experience whereas if students indicated a strong desire, one could focus more on provision of additional context and proposed steps to take their learning further.

When asked about existing knowledge in cyber security, most undergraduate students identified as having knowledge from modules previous studied within the programme. Some identified as not having been taught anything on security, which highlighted how some students cannot recall consideration of security within non-security focused modules. A small number of responses mentioned exploring online information through websites such as YouTube. Most of the topics identified were awareness of basic cryptography, web security and hash functions.

Students completing the Masters module, the majority identified as having no existing cyber security experience. Those who did appear to have gathered this from online sources and textbooks rather than formal studies. This is perhaps unsurprising given that this is a module on a conversion programme and as such this is aimed at students with no computing science background.

4.2 Topic and Skills Expectations

In the computer security module when asked about topics students would like covered in the module, answers mainly focused on cyber security as it relates to programming. In particular students wanted to be sure how to write "secure" code. This was reflected in both 4th year Computer Security and Enterprise Cyber Security with comments along the lines of "how to do it", "how it works" and "secure coding". Whilst this was also reflected in the answers from Enterprise Cyber Security students, answers also covered aspects of law and related regulations. This is perhaps reflective of this cohort's background.

Students also commented on how important they felt it was to have "real world" or "practical" security taught to them. However, students often failed to articulate what this meant to them more precisely. In spite of this lack of specificity there was a clear perception that students believed cyber security is taught from only a theoretical perspective at University and this warrants attention.

A range of answers were provided when students were asked which skills they thought were important for cyber security practitioners. The most common of which were as follows, the total count of occurrences across both cohorts is shown in brackets:

- understanding of up to date techniques (48)
- strong programming skills (34)
- communication (25)
- attention to detail (19)
- problem solving (19)

Answers across both Computer Security and Enterprise Cyber Security reported similar mentalities and perceptions. It was interesting that the second most common theme was that of strong programming skills, which is not necessarily in line with many of the roles in cyber security which can be less focused on secure coding, and more on analysis of systems security or organisational policies and procedures.

4.3 Perceptions of Future Usefulness

Students perceptions of future use tended to fall into one of three categories as follows; I will not be seeking a security role so it is not needed, it is always important, and it is very important as I want to work in a related field. The majority of responses identified that the student perceived security as highly relevant and important. A total of 92 students identified it as being an important aspect no matter which role they pursued. Nine students were unsure of how it might play a role in their future career. 16 students identified it as very important as they wanted to pursue a career in the field and three explicitly identified it as not relevant or important to them as they were not pursuing a job in the field. It was reassuring to note that almost all students identified it as being important, even if they did not foresee have a security focused role.

5 DISCUSSION AND RESPONSE

It was clear from responses that many students had an idea of what cyber security means for them. This often took the form of secure programming as evidenced through the responses to what they want to learn, as well as the skills required where programming was the second most frequently mentioned. There was also a clear desire for cyber security to relate to the "real world". Students appeared to perceive that cyber security taught at University is often theoretical. This perspective is likely expected by lecturers who teach security. It is perhaps reflective of the need to better address student expectations and clarify how aspects which may seem theoretical are applied in real world security.

Topics which students wanted to cover in the modules included more detail on cryptography, ethical hacking, secure coding, and web security. Some students were not able to articulate their expectations e.g. participant 100 said they wanted to learn "enough".

In terms of the skills students believed were required, programming was second only to current knowledge. This is somewhat contrasting to the wide range of roles which a cyber security specialist can have, many of which do not involve secure coding. Whilst a proportionally small number of 4th year students (8/125) identified as wanting to pursue a career in cyber security, the majority of students recognised the importance and relevance to all careers.

As a result of the activity, both module leads reflected on responses for their cohorts and considered a longer term development of module content in order to better reflect student expectations. Additionally, a micro intervention was implemented in the 4th year module for the cohort who completed the survey reported here.

This was applied specifically to the 4th year module as this feedback was particularly prevalent for this cohort. Given the small proportion of the Masters cohort who responded (around 16%) the decision was taken to reflect over a longer period before curriculum changes were implemented.

Whilst not co-creation, students responses did impact on delivery of the curriculum for the 4th year class. A micro intervention involved finding a recent news article which related to the module content and presenting this at the start of each week. These were selected with the intention of more clearly articulating how 'theoretical' elements were practically embedded in the real world. For example, in a week discussing cryptography and the RSA algorithm, a news article describing how Windows 10 makes use of RSA to encrypt solid state drives was presented to students.

Upon completion of the module, students were then surveyed on whether the news articles increased the meaningfulness of the content of the module. Students were given the options of not at all, somewhat or definitely. Approximately 76% of students who responded (16 out of 21) noted at least some increase in meaningfulness of content due to the use of real world current cyber news. Around 38% noted a clear increase in meaningfulness. One limitation to note, is that those who responded not at all may already recognise the relevance of the content. Further examination would be required for a more definitive response on whether this was the case, however on balance the intervention appears to have had some positive impact on the student experience.

Since running the activity, longer term adjustments to curricula for both modules have been made. For example, in the 4th year module a number of long term curricula changes have been made. This includes developing secure coding material and practical exercises which was a clear expectation from those students. Additionally, module content is continually refreshed to better reflecting recent developments in cyber security, established through consultation with industrial contacts who work in cyber security roles. A further evaluation to determine the effectiveness of these changes is required, however it is worth noting that the comments on the module not being clearly practical now do not appear in student feedback, some comments go further and note how valuable they find it to see how concepts such as (a modified) Diffie-Hellman key exchange is used in real world situations such as in the secure messaging application Signal. There are a number of limitations of this work which should be highlighted. An in-time intervention was only applied in one module. Ideally this would have been across both modules. However, longer term adjustments have since taken place across both modules. It might have been more valuable to implement more significant module changes at the time of delivery, however timing was such that significant changes were infeasible. A more structured approach to analysing the feedback may have also been helpful, such as more structured thematic analysis. It would also be helpful to repeat the survey in order to better track changes over a longer period of time. Similarly, feedback on the effectiveness of interventions would be improved by a more significant formal evaluation. Moving forward the aim is to develop this further by adjusting the survey to make it more lightweight. focusing more on expectations and exploring ways to co-create module content to meet those expectations.

6 CONCLUSION

In this paper a structure for exploring student expectations and experience with regards to cyber security was presented, alongside two micro interventions which could be deployed to increase perceived relevance and address student expectations. It was felt this activity was valuable in helping students reflect on their experiences and start a dialogue to better identify and manage expectations of security modules.

Whilst two micro interventions were presented as a result of the survey, it is recognised there are many more ways of achieving this. Discovering students expectations and understanding of cyber security and being able to relate the material to these expectations in a meaningful way was found to be helpful in engaging students more fully. It is hoped some of these approaches will be explored more in future by other cyber security educators, thus helping to bridge the cyber security skills gap.

REFERENCES

[1] BCS. 2022. Academic Accreditation Guidelines. (2022). https://www.bcs.org/media/1209/accreditation-guidelines.pdf

[2] Andrew Begel and Beth Simon. 2008. Novice Software Developers, All over Again. In *Proceedings of the Fourth International Workshop on Computing Education Research* (Sydney, Australia) *(ICER '08)*. ACM, New York, NY, USA, 3–14. https://doi.org/10.1145/1404520.1404522

[3] Tom Crick, James H. Davenport, Paul Hanna, Alastair Irons, and Tom Prickett. 2020. Overcoming the Challenges of Teaching Cybersecurity in UK Computer Science Degree Programmes. In *2020 IEEE Frontiers in Education Conference (FIE)*. 1–9. https://doi.org/10.1109/FIE44824.2020.9274033

[4] Sebastian Dziallas and Sally Fincher. 2019. Accountable Disciplinary Knowledge in Computing Education: A Case-Comparative Approach. In *Proceedings of the 2019 ACM Conference on International Computing Education Research* (Toronto ON, Canada) *(ICER '19)*. ACM, New York, NY, USA, 1–9. https://doi.org/10.1145/3291279.3339403

[5] The Quality Assurance Agency for Higher Education. 2022. Subject Benchmark Statement- Computing. (2022). https://www.qaa.ac.uk/quality-code/subject-benchmark-statements/computing

[6] UK Government. 2016. National Cyber Security Skills Strategy: Increasing the UK's Cyber Security Capability. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021. [Online: accessed 14-October-2022].

[7] U.K. Government. 2016. National Cyber Security Strategy 2016-2021. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021. [Online: accessed 14-October-2022].

[8] U.K. Government. 2018. Defining the cyber security skills gap. https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/706/70605.htm. [Online: accessed 14-October-2022].

[9] Hiscox. 2019. 2019 Cyber Readiness Report. https://www.hiscox.com/cybersecurity. [Online: accessed 14-October-2022].

[10] Päivi Kinnunen, Matthew Butler, Michael Morgan, Aletta Nylen, Anne-Kathrin Peters, Jane Sinclair, Sara Kalvala, and Erkki Pesonen. 2018. Understanding initial undergraduate expectations and identity in computing studies. *European Journal of Engineering Education* 43, 2 (2018), 201–218. https://doi.org/10.1080/03043797.2016.1146233

[11] NCSC. 2016. CyberInvest. https://www.ncsc.gov.uk/information/cyber-invest. [Online: accessed 14-October-2022].

[12] Donna M. Ogle. 1986. K-W-L: A Teaching Model That Develops Active Reading of Expository Text. *The Reading Teacher* 39, 6 (1986), 564–570. http://www.jstor.org/stable/20199156

[13] Cybersecurity Ventures. 2021. 2021 Cybersecurity Jobs Report. https://cybersecurityventures.com/jobs/. [Online: accessed 14-October-2022].

[14] Rossouw von Solms and Johan van Niekerk. 2013. From information security to cyber security. *Computers and Security* 38 (2013), 97 – 102. https://doi.org/10.1016/j.cose.2013.04.004 Cybercrime in the Digital Economy.