To evaluate the effectiveness of focused staff training in recruitment on specialised modules

eSTEeM Final Report

Phil Hackett, Anthony Johnston and David McDade (Project lead)

Keywords: Staff development; cybersecurity; upskilling; specialist modules

The Open University

eSTEeM
Centre for Scholarship and Innovation
Science, Technology, Engineering and Maths

Contents

Executive Summary

Skills shortages outlined by the Department for Digital, Culture, Media & Sport (DCMS) and the Department for Science, Innovation and Technology (DSIT), determined the backdrop for the development of the BSc Cyber Security R60 qualification.

Within the School of Computing and Communications (C&C), recent updates to the curriculum have also highlighted issues around 'skills gaps' and the impact this is having on tutor recruitment. Examples of this are the introduction of new specialist modules TM256: Cyber Security and TM359: Systems Penetration Testing, both of which have been introduced as part of the new R60 BSc (Hons) Cyber Security qualification[1] both of which have proved hard to recruit to.

The school has sought to address this by offering training in specialist areas in a bid to increase the expertise of the tutor community. This training has taken place through offering specialist cyber security training courses available from Cisco and The International Council of E-Commerce Consultants (EC-Council).

This has allowed tutors to upskill into areas of cyber security and to develop confidence in applying for cyber security related modules, whilst gaining industry recognised professional certification. It has also allowed the school to meet (and extend) the quotas for high demand modules.

[1] R60 BSc (Hons) Cyber Security

An investigation took place into how recruitment of tutors on specialised modules could be assisted by the provision of focused staff training. The objectives for the project were to determine:

- To what extent is focused staff training effective in the recruitment of tutors?
- What approaches and resources are required to upskill tutors?

A survey was distributed to 110 tutors who had enrolled on CPD training. There was a 40% return rate.

The majority of the tutors surveyed would have been willing to do the CPD training in their own time and would not have applied to tutor on the specialist module without completing the CPD. The strong mapping between the information taught and the content on the module helped the tutor to feel confident to apply for a position. The fact that the CPD on offer was supplied by a vendor was also important for the tutors in going on to apply to teach on the module and may also have been influential in the tutors agreeing to do the CPD. The training increased confidence regarding the subject matter.

Having to pay for training oneself would have been a barrier for the vast majority (94%) of the tutors. Tutors found working to a deadline to complete the training off-putting, but it is hard to see how this could be avoided.

Tutors who started the training in Spring or Autumn were nearly twice as likely to complete the training than those who started in July and this should be considered in the timing of any future CPD.

Future work included the development of multiple packages of CPD for different curriculum areas within the School and the approach of offering CPD to existing tutors in specialist areas such as AI and machine learning is now a high priority.

Recommendations

It would be useful for other faculties to create 'specialist' resources within the MyLearning Centre space to support their own curriculum areas.

There are resources already available within the C&C MyLearning Centre space that other curriculum areas my find useful (e.g. programming resources).

Consideration should be given to the timing of future CPD events.

Aims and scope of the project

Rationale for the qualification

According to the Department for Digital, Culture, Media & Sport (DCMS) during 2022 a significant proportion of businesses in the UK reported that they continued to lack staff with a range of fundamental cyber security skills such as governance, technical, and incident response skills. Approximately 51% have a basic skills gap, 33% have advanced skills gaps and almost 37% have specialist internal skills gaps. (DCMS, 2022)

This trend continued into 2023 in an updated government report published in June 2023 by the Dept. of Science, Innovation and Technology (DSIT). This highlights that around 50% of businesses still have a basic skills gap. (DSIT, 2023)

The R60 qualification was designed and conceived under this context, using references from national cyber security frameworks, such as: The Institute of Information Security Professionals (IISP)[2] and The Cyber Security Body of Knowledge (Cybok)[3]. These frameworks ensure that the new qualification meets industry needs as well as standards.

Educational aims

The R60 qualification is seen as key to positioning the University as an employment-focused and research informed institution in the cyber security education arena. This

[2] The Institute of Information Security Professionals
[3] The Cyber Security Body of Knowledge

allows the University 'to make a positive impact on the economy, society and culture of the United Kingdom and beyond, through innovation and engagement'. (OU, 2020)

The qualification aims to provide graduates with a wide range of cyber security as well as academic related abilities:

- To evaluate tools (e.g. nmap, and wireshark) and techniques (e.g. phishing and social engineering) at the forefront of the discipline.
- Critical analysis and application of concepts, principles and practices in cyber security.
- Undertake related projects to professional industry recognised standards.
- Recognition of legal, social, ethical and professional issues in cyber security.

Qualification and curriculum development

During the learning design process, a curriculum mapping exercise took place to identify cyber security gaps in the current Q62 BSc (Hons) Computing and IT[4] framework. This was then compared against the CyBOK framework. This identified a relative coverage of basic cyber security topics throughout levels 1, 2 and 3 within the School. The existing topics (when combined) were adequate enough for coverage of cyber security at level 1. Gaps, however, were revealed at levels 2 and 3, which lacked relevant detailed topics. As a result, the R60 qualification was now to include two new mandatory modules: TM256: Cyber Security at level 2 and TM359: Systems Penetration Testing at level 3 (please see Appendix 1 for the R60 qualification map).

[4] OU: BSc (Hons) Computing & IT

Activities

Identifying risks

During the development of the module specifications for TM256 and TM359, a number of risks associated with the modules were identified. One of the risks was the ability to attract sufficient tutors with relevant experience. For TM359 there were also risks associated with having only one module team member with the required specialist skills, subsequently leading to a high-level of dependence on a single member of the module team. Response actions go on to identify that funding mechanisms could be used to support existing tutors to study cyber security related courses to 'upskill' for teaching on the module.

Existing skills within the school

In identifying existing areas of cyber security during the curriculum mapping exercise, this also allowed for identification of staff with existing skills that would be suitable for teaching on the new cyber security modules. At level 1 there are a number of tutors familiar with the basics of cyber security as it is taught on modules TM111 and TM112. TM129 was identified as having intermediate elements (as part of Block 1 Networking).

At levels 2 and 3, there are 'pockets' of cyber security skills across the curriculum, for example Information Security (TM311) and more advanced level network security through Cisco CCNA based modules TM257/TM357.

Although this has identified tutors capable of teaching on new cyber security modules, the school felt that there was still a need to provide training that was capable of providing a 'broader brush' of cyber security skills to tutors within the school. Concerns also remained around the highly specialised skills needed for teaching on TM359.

Identifying training – mapping training to module outcomes

By this stage the structure and the topics contained within TM256 had been established and the decision was taken to use the Cisco Network Academy (NetAcad) platform and course 'Cyber Security Essentials' as a means of providing upskilling. This is a 30-hour course, where a significant amount of course material (around 85%) mapped to TM256.

For TM359, an existing alliance between the OU and the EC-Council[5] exists that allows university staff full access to the Certified Ethical Hacker (CEH) material and the associated iLab environment. TM359 is aligned to the EC-Council CEH certification and tutors undertaking training would complete the course, providing them with necessary skills and knowledge (and practical ability) to teach on the module.

Existing Literature

Providing teaching staff with the skills required to teach specialist courses remains a widespread problem, not just at the Open University, but across the UK education sector. For example, a recent report published by Education Scotland highlights the importance of having highly skilled teaching staff within schools who are able to work meaningfully within the digital (cyber) arena ensuring that 'Cyber resilience internet safety concepts are progressively taught and revisited throughout teaching and learning.' (Education Scotland, 2022)

The lack of cyber security skills in education, as well as industry, is identified by Blažič (2021) as a problem that exists globally and not just in the UK and Europe. Blažič

[5] EC-Council

discusses that the recruitment, retaining and maintaining of cyber security professionals in the workplace and academia is an ongoing battle.

Blažič identifies a number of issues. One of the difficulties is that existing HEI cyber security programmes are too focussed on 'traditional' technical cyber security topics and fail to deliver the range of skills required in contemporary cyber security arenas. Also, the demand for cyber security skills in industry is such that academia cannot attract relevant academics with knowledge, experience, research background and academic aspirations.

Discussion shifts to the use of computing vendor certifications and studies that have taken place in the recent years in the US. These studies discuss proposals for improving the current situation around skills gaps. In this, we see addition of vendors and agencies such as Cisco, CISSP (Certified Information Systems Security Professionals) and CISA (Cybersecurity and Infrastructure Agency). They propose a simple model where after completion of an academic qualification, candidates complete a general cybersecurity professional certification and then complete a more cybersecurity technology specific qualification.

The paper also discusses the importance of attributes of 'traditional' computing science teachers and how the possession of skills such as data communications, encryption, secure coding and operating systems can contribute to the delivery of effective cyber security teaching.

The paper concludes that the answer is to enrich current HEI curricula with focused content from specific knowledge areas, including content that is least covered such as human aspects of cyber security. Training and building of skills can be offered either as part of own installations of HEI frameworks or by cooperation with additional vendors.

A journal article from 2021 on increasing teacher competence in cybersecurity (Kuzminykh *et al.*, 2021) discusses in greater detail the need for and development of cybersecurity educators and the role they play in helping educate students in the face of growing cyber-attacks across Europe (in particular, Eastern Europe). This report proposes that three approaches can be taken to develop professional competence:

- Group training – focusing on delivering face-to-face training programs to university teachers.
- Individual training (using mentors) – improving teacher expertise in one specific area and allowing for alignment to teacher competence frameworks.
- Self-education – enhancing proficiency through participation in targeted programmes of study, reading, watching or listening to materials relevant to their subject of interest.

The models outlined above have been chosen for inclusion as they are very similar to the approaches taken in this study whereby academic teaching staff have been allowed to enter onto focussed training schemes to allow them to upskill into specialised areas to allow effective delivery of new curriculum.

OU Staff Development policy recognises that the success of the university 'depends on all staff whatever their role having the relevant skills, knowledge and competencies to support the strategic priorities now and in the future'. (OU, 2022) The policy identifies a number of points around the general principles of staff development; however, the policy seems to mainly focus on organisational aspects and the role the CDSA process plays in identifying the needs of staff as well as the responsibilities of line managers. Although the policy briefly mentions module planning and review, it makes no mention of the risks set out by qualification related documents and the role that suitably skilled staff plays in effective module development and delivery.

Additionally, although the OU provides opportunities for staff development through, for example, the staff fee waiver scheme (OU, 2023), there does not seem to be any [formal] scheme in existence that provides a focussed approach in order to address specific gaps in skills such a cyber security.

The following word cloud represents a snapshot of comments from tutors that participated in the survey that examined the impact of this training scheme. Results of this survey will be examined in more detail in the next part of this report.

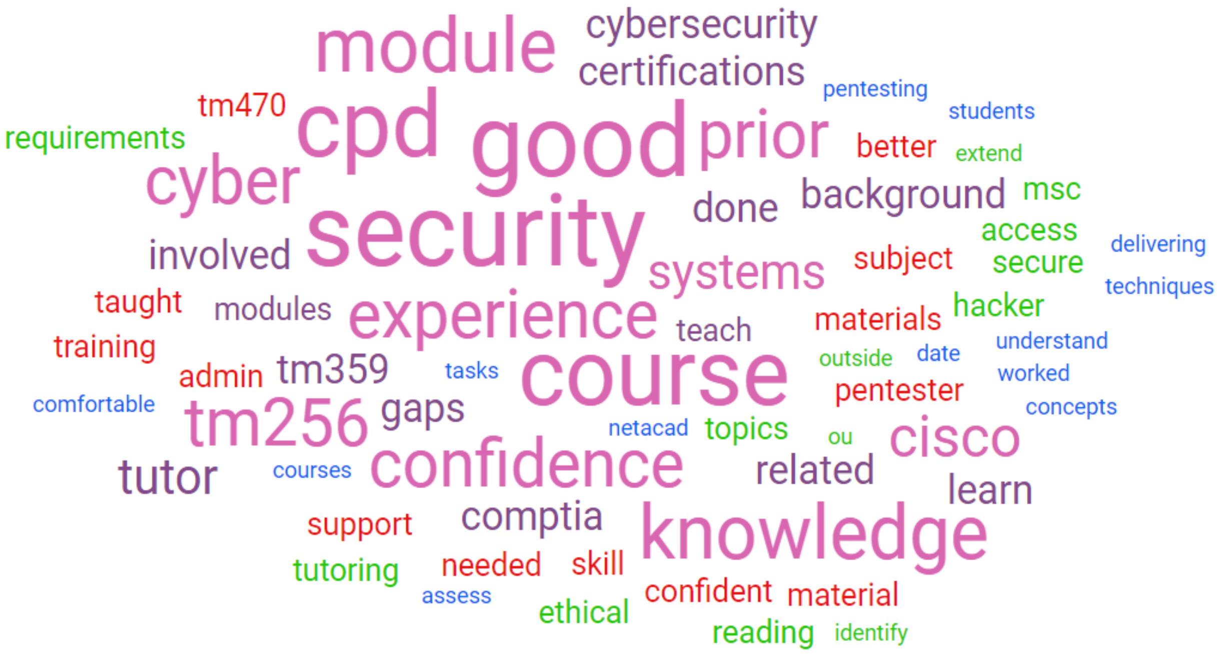


Figure 1: *Word cloud of survey comments.*

Findings

Research Questions & Method

Following the offer, to C&C tutors, of focused CPD (continuous professional development) relating to Cyber Security, we wanted to assess the impact in terms of tutor recruitment for the specialist modules (TM256 Cybersecurity and TM359 Systems Penetration Testing) as well as assess the potential success and viability of this approach with other OU modules.

We started with the following research questions:

- To what extent is focused staff training effective in the recruitment of tutors for specialised modules at levels 2 and 3?
- What approaches are required to upskill tutors to successfully tutor in specialist curriculum areas?
- What resources are required to upskill tutors to successfully tutor in specialist curriculum areas?

We then used Jisc Online Surveys to design a quantitative and qualitative survey, containing a mixture of Likert and free text questions. We used Likert scale questions to ascertain:

- How helpful certain aspects of the CPD were? (e.g. Setting a deadline for completion)
- How influential certain aspects of the CPD were on the tutors deciding whether to apply to tutor on the modules? (e.g. Sponsorship payment)
- Impact on tutor confidence in tutoring certain module topics

We also used the free text responses to gather additional detail regarding tutor responses. The questionnaire can be found in Appendix 2.

Our survey was targeted at the tutors who had participated in the CPD offers. We also sent the survey to tutors who did not participate in the CPD, but who were current TM256 or TM359 tutors. In total, we sent the survey to 110 tutors with a 40% response rate. The responses of those tutors who participated in the CPD were split into 3 different groups:

Cyber Security Essentials (TM256) sponsored tutors – 1 day ADC (additional duties contract)
Cyber Security Essentials (TM256) non-sponsored tutors
Certified Ethical Hacker (TM359) sponsored tutors – 2 days ADC

The key points ascertained from the survey included identifying the following:

1. the main influences from doing the CPD that led the tutor to apply to teach on one of the modules;
2. if tutors would be willing to do CPD in their own time (without payment);
3. whether a tutor would have applied to tutor on the module (TM256 or TM359) without having completed the CPD.

Tutors were asked to select the factors influencing their determination to apply to be a tutor on either TM256 or TM359 from a list. The single biggest influence (Chart 1) is that the CPD provided was module specific and beneficial to tutoring on the respective modules. The next biggest influence was the vendor – the fact that these are industry recognised CPD from well know vendors. The fact that sponsorship of 1- or 2-days Additional Duties Contract (ADC) was provided was also influential, however Chart 2 shows that 74% would be willing to do the CPD in their own time.

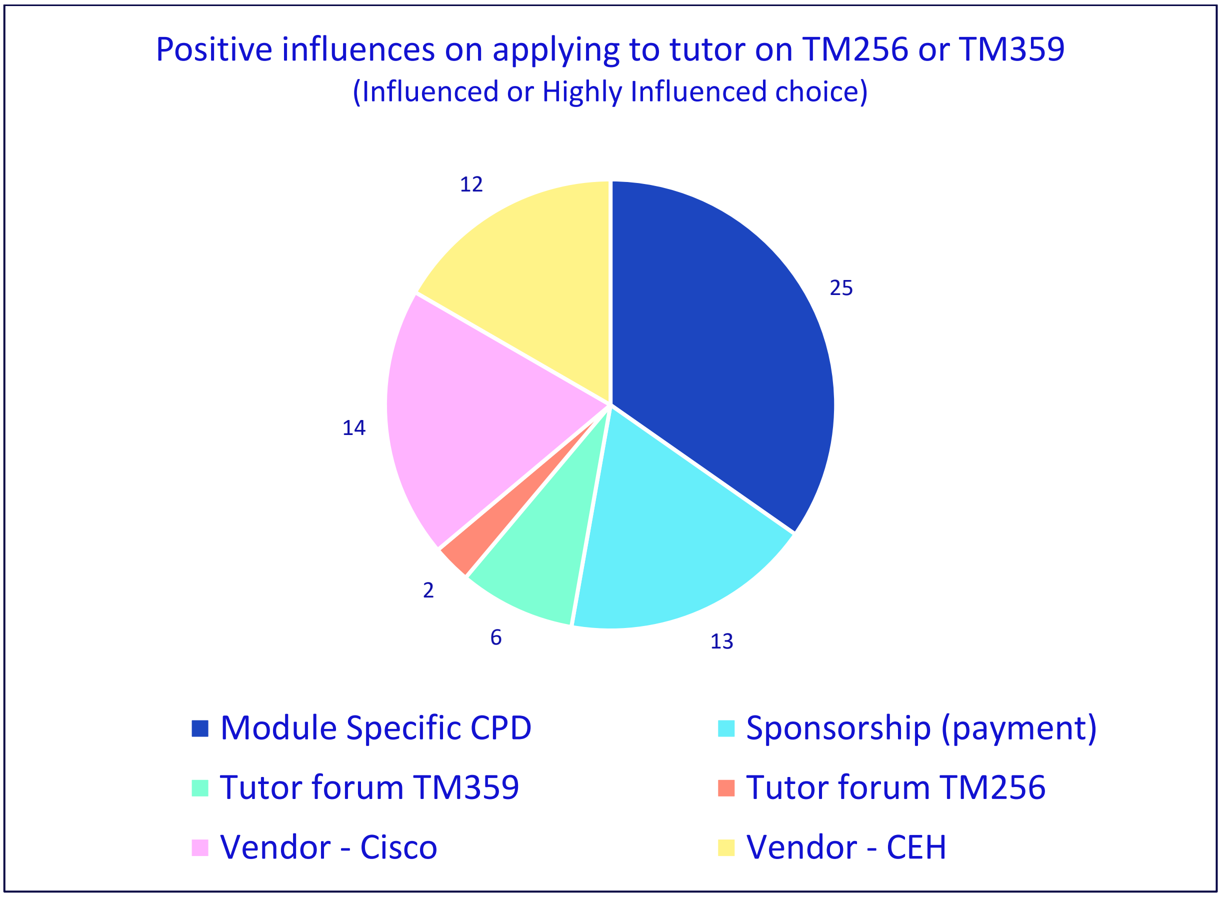


Chart 1: *Positive Influence*

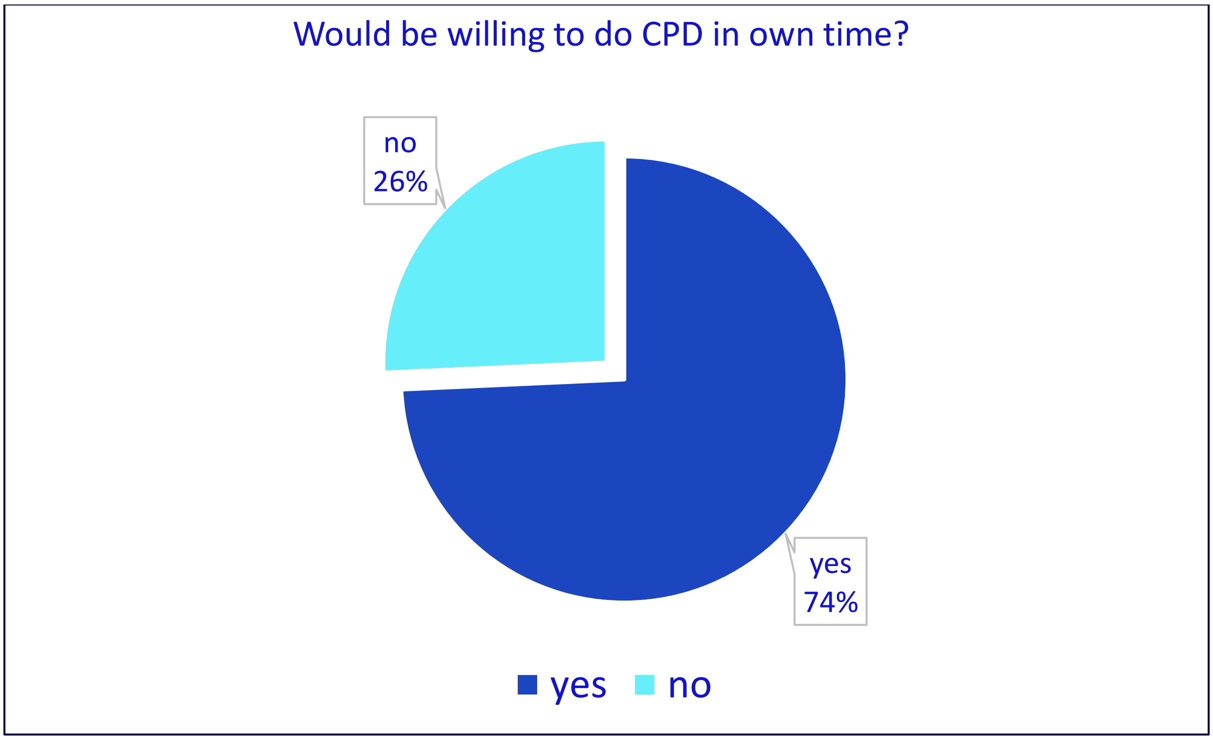


Chart 2: *Willing to do CPD in own time (without payment)*

One of the most important aspects that we identified is shown in Chart 3. Two thirds of tutors would not have applied to tutor on the module without completing the CPD. We may have struggled to recruit enough tutors without the CPD offering.

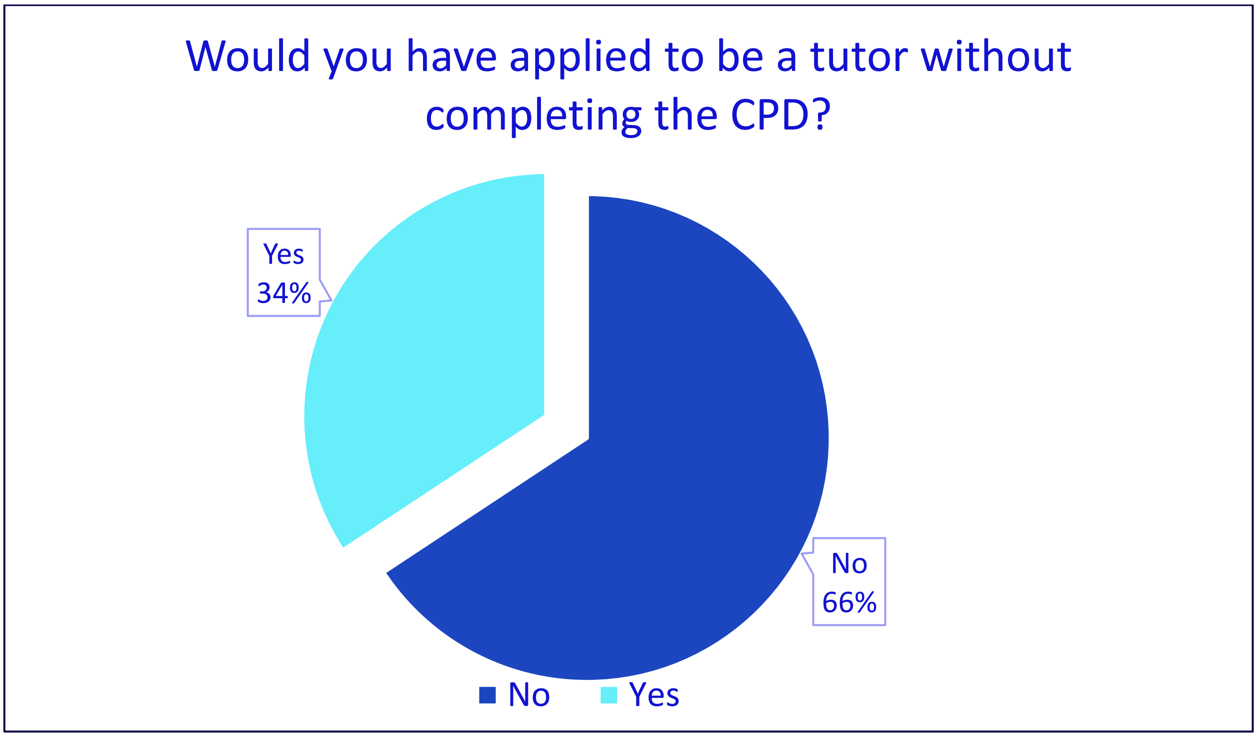


***Chart 3**: apply to be a tutor without completing the CPD?*

Discussion

The questionnaire was distributed to 110 tutors who had enrolled on either the Cisco Cyber Security Essentials or the Certified Ethical Hacker courses; of these, 44 tutors returned a completed response representing a 40% return rate. This is a relatively high rate, and it could be that tutors were motivated to take part in the survey as it was specifically stated that the questionnaire would be used to evaluate the training and feed into future offerings. In other words, those who had benefitted from the training may well have been motivated to return the questionnaire as a step to ensure that future training would be offered.

Of those who responded, there were ten tutors who did not compete the course they were enrolled in; they were asked if there were specific reasons for that. Of those, six (60%) cited a lack of time and two (20%) stated they did not like an aspect of the course. The failure to complete due to lack of time is a problem when it comes to offering CPD in an organisation. However, of the 105 enrolments on the courses, 71 did complete (67.6 %).

It has already been stated that the biggest influence on whether a tutor went on to apply for a position on one of the target modules (TM256 or TM359) was the fact that the CPD offered was specifically chosen to help the tutor gain confidence to teach on the module in question. It could be concluded that specific training of this kind is very much welcomed by tutors and, at least in this case, the strong mapping between the information taught and the content on the module helped the tutor to feel confident to apply for a position. Tutors who want to be trained to teach on specialist modules are more likely to apply for training, complete the training and subsequently apply to teach on the specialist module if they are confident that the module material has been covered. Knowing that the material is also mapped to, or supplied by, a vendor may well help with this perception. Indeed, the fact that the CPD on offer was supplied by a vendor was also important for the tutors in going on to apply to teach on the module.

This could have been because of the additional credence given to the CPD material. The tutor may also have been influenced in taking the training because they would complete it with a recognised qualification, useful to them in their employment outside the University.

Because of the way that funding was available when groups of tutors took the training, some were given payment for their time while others were not. None of the tutors had to pay for the training. Tutors participating in the CEH training also had the opportunity to take the CEH exam, using a voucher that would allow one attempt, without cost. 18% of those who went on to apply for a tutor position said they were influenced by being sponsored for their time, so this was a factor. However, as mentioned earlier, 74% of the tutors would have been willing to do the training in their own time. On the other hand, only 6% of the respondents would have been willing to have paid for the training themselves.

The Open University was fortunate to have partners who could provide the CPD training with no extra cost to the university. Having to pay for training oneself would have been a barrier for the vast majority (94%) of the tutors.

Regarding the content of the CPD courses, tutors were asked if they found each of the following helpful or not in their studies:

- Practical activities (Labs)
- Written Materials
- Video Materials
- Deadline for completion
- Use of a Forum (with other tutors doing CPD)

The result of this question is summarised in the pie-charts below (charts 4 and 5). The aspects of the content seen as most helpful were the written and video materials (more than a quarter of the tutors said they found these helpful or extremely helpful). Perhaps surprisingly just 8% said the same of the forums and while 15% said they found the deadline helpful or extremely helpful, 35% said that the deadline was not helpful or not at all helpful.

This negativity toward a deadline is difficult to mitigate in the sense that the University needed the tutors to finish their training in time to teach on the modules. One piece of future work might be to help tutors to understand the need for a deadline and to use it to their advantage. It can be a motivational factor to have a target date which one is working toward as long as there is perceivable progress (Katzir, et al., (2020).

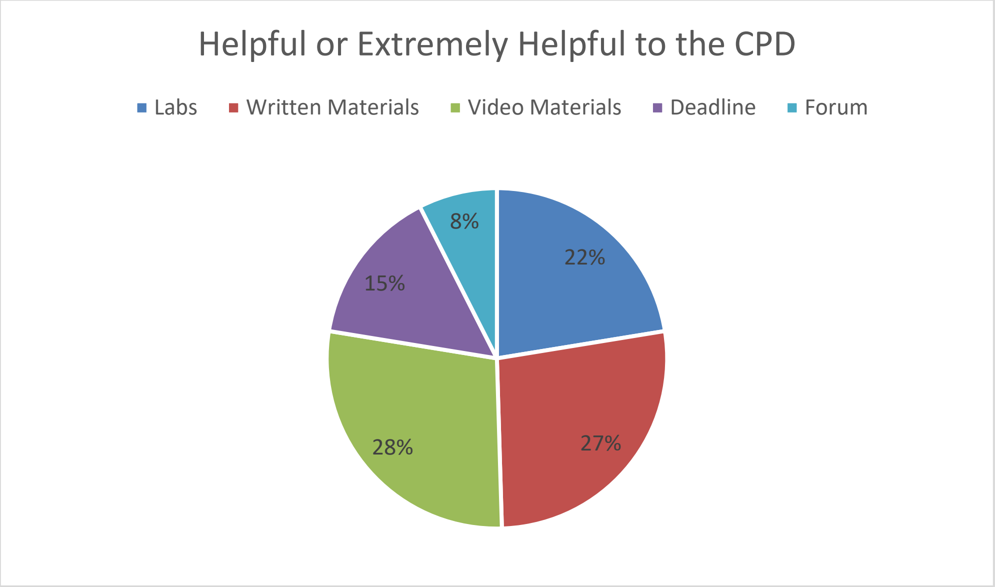


Chart 4*: content seen positively by tutors*

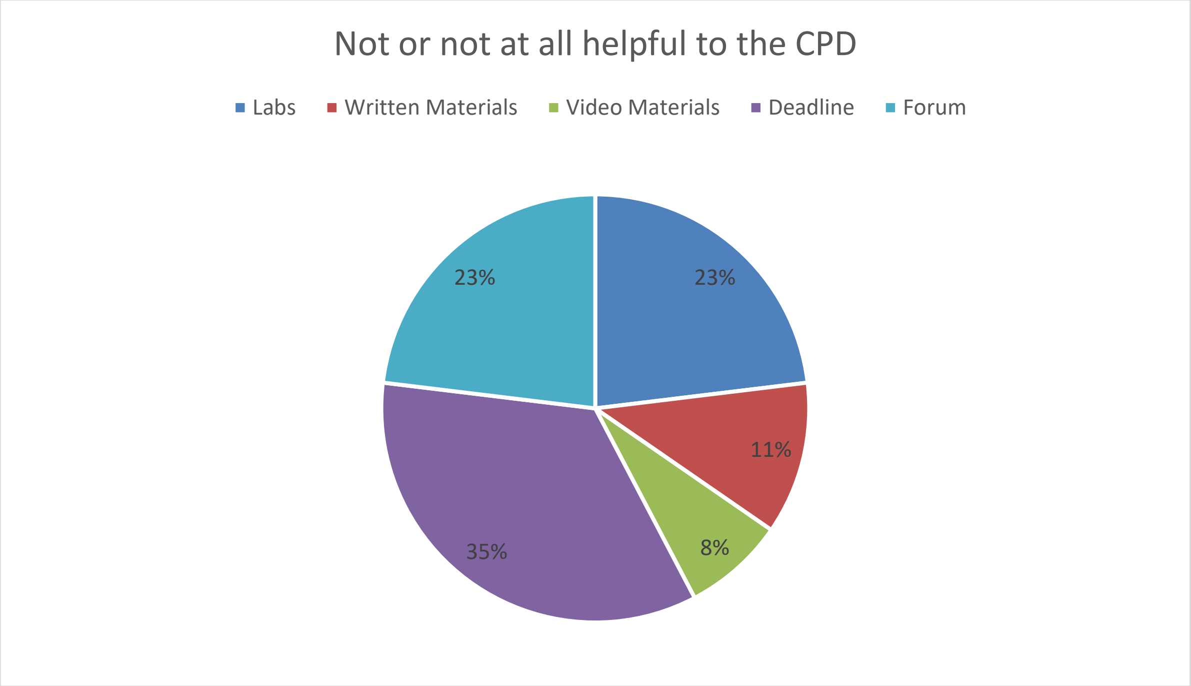


Chart 5: *content seen negatively by tutors*

One factor that may have influenced whether a tutor completed or not was when the training started and if it ran over the summer or not. Some of the training packages ran in the spring or autumn and generally these ones were completed at a higher rate than those that started in July. (78.8% of those who started in March, May or September completed as against 48.7% of those who started in July). It seems that in this case, at least, it is helpful for tutors to start training at a time of year that suits them and not just before a holiday period. Many of the tutors would be taking a break over the summer and this may well have interrupted their studies sufficiently that they were unable to get back on track.

It is possible to use the results of the questionnaire to explore the confidence of tutors while teaching on the module. Chart 6 shows how confidence levels changed for those who completed the training. For both sets of training (Cyber Essentials and Ethical Hacking) the number of tutors who were confident or very confident regarding the module subject matter increased significantly. For those doing the Cyber Essentials, the number of those who had little or no confidence fell from 7 to zero, and for those studying Ethical Hacking, the number fell from 11 to 1 (and the one remaining reporting having "little confidence" rather than "not at confident").

It can be concluded that the training increased the confidence regarding the subject matter.

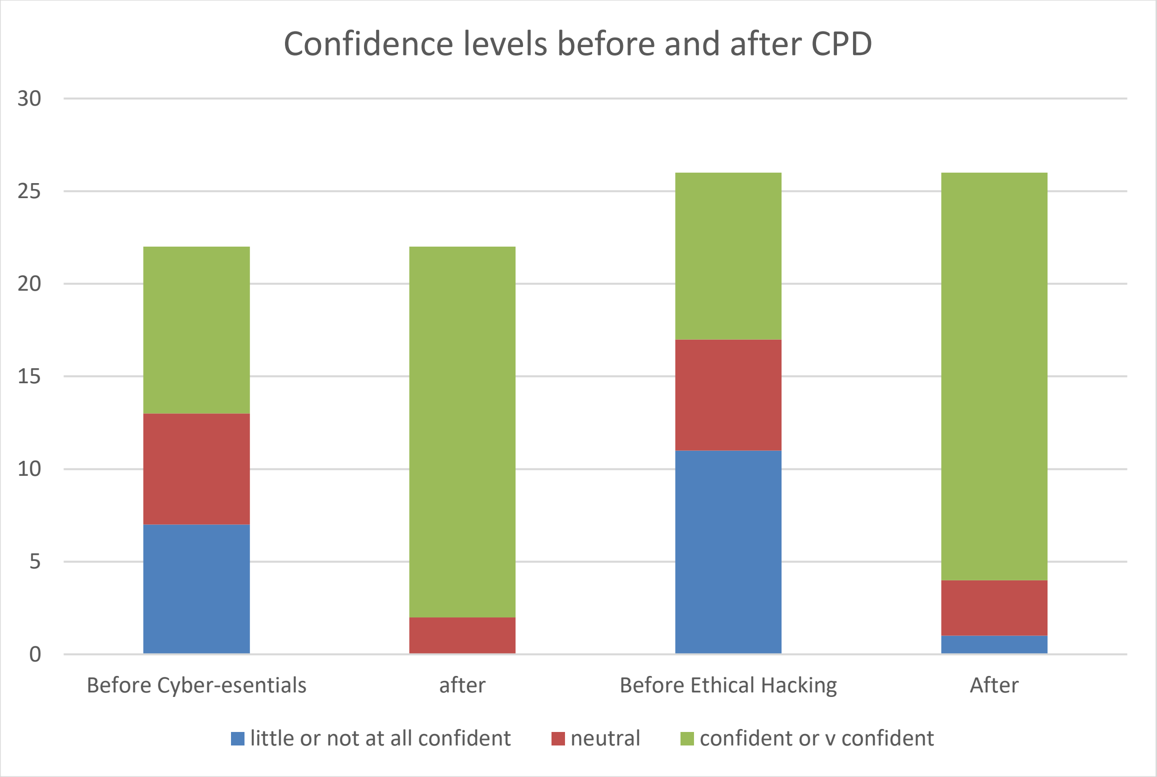


Chart 6: *Confidence levels before and after taking CPD*

One set of questions asked tutors how confident they feel teaching on each block of the module. This question was asked to tutors who had done the CPD and those who hadn't done the CPD (both sets of tutors having gone on to teach the module). There is little difference in response rates to the questions and a more or less equal spread of answers. It can perhaps be concluded that those who went through the CPD ended up with similar confidence levels to those who gained their experience through industry.

Of the three approaches to increasing competence in teaching cybersecurity that were mentioned by Kuzminykh and discussed earlier, self-education is the closest to the approach taken in the delivery of CPD. The survey indicates that the approach has been shown to be successful.

Future Work

There are plans for the development of multiple packages of CPD for different curriculum areas within the School of C&C. A pilot has already taken place with a Software Development module (M269), which is a ‘difficult to recruit to’ module. The approach of offering CPD, to existing ALs, in specialist areas such as AI and machine learning is now a high priority for the school and the university.

A dedicated page for all this CPD will be located on the My Learning Centre facility, which includes the ability to generate completion certificates and integrates with the academic record (ALAR) of Open University Associate Lecturers.

Conclusions

When designing Continuous Professional Development courses, subject matter which is module-specific or content-specific material and so matches a module is important. Tutors are much more likely to be motivated if their perception is what they are studying is matched to the content of what they will be teaching.

Tutors are motivated to complete training if the content is linked to a Vendor as they will obtain a qualification that holds currency outside of the educational establishment, in other words in industry.

Although free training is important to tutors, they would not object to completing the training in their own time if they can see the advantages of doing so.

Impact

a) **Student experience**

- This project has had impact on student learning as it has enabled tutors to upskill into contemporary areas of cyber security, allowing them to deliver an up-to-date learning experience for students.
- As a result of training, tutors are able to deliver teaching that is of relevance in the real-world.
- It allows tutors to deliver the foundational skills that students need to progress to advanced level cyber security courses on the R60 qualification.
- The training allows tutors to deliver improved digital safety for students and raise awareness of cyber security in the context of wider digital citizenship.

b) **Teaching**

- Through this project, we have been able to influence the practice of others by developing the workforce in order to effectively deliver the R60 qualification.
- This project has had the impact of allowing subsequent development of a training platform for OU teaching staff, through My Learning Centre (not just for C&C).
- Outside of the OU we have been able to share information with external partners (such as Cisco) on how we have used computing vendor awards to upskill OU tutors and the positive impact it has had.

c) **Strategic change and learning design**

- This project aligns to STEM Strategic plan 23/24 – 27/28 (OU, 2024)
    - Deliver a Positive, Consistent and Inclusive Student Experience
    - Deliver the STEM curriculum plan (deliver new curriculum)

- The project has had huge impact in terms the R60 qualification being able to meet and surpass student quotas (mainly for module TM256: Cyber Security).
- TM256: Cyber security maintains an average pass rate of 75% with completion to pass rate of around 95% and retains on average 82% of students.

d) **Recommendations**

- External resources are of benefit and can be put to use for the development of OU teaching staff.

Dissemination

Deliverables

eSTEeM conference poster (March 2023)

Staff development presentation to C&C Staff Tutors (May 2023)

eSTEeM conference presentation (April 2024)

AL conference presentation (November 2025)

STEMinar presentation (March 2025)

Figures and tables

List of charts

References

Blažič, B.J., 2022. Changing the landscape of cybersecurity education in the EU: *Will the new approach produce the required cybersecurity skills?*. Education and information technologies, 27(3), pp.3011-3036.

Cisco Networking Academy (2022), *Skills for All with Cisco Networking Academy: Networking Essentials 2.0.1 Scop and Sequence*. Available at: https://www.netacad.com/sites/default/files/ss-netess.pdf (Accessed September 2023).

DCMS (2022). *Cyber security skills in the UK labour market: Findings report.* Available at: https://tinyurl.com/23nn8mxu (Accessed February 2023).

DSIT (2023). *Cyber security skills in the UK labour market 2023: Findings report.* Available at: https://tinyurl.com/3uzvtbdv (Accessed August 2023).

Education Scotland (2022). *Features of Highly Effective Digital Learning, Teaching and Assessment in Schools.* Available at: https://education.gov.scot/media/cxwnqrma/nih312-features-of-highly-effective-digital-learning-and-teaching-01-22.pdf (Accessed September 2023).

Katzir, M, Emanuel, A., Liberman, N. Cognitive performance is enhanced if one knows when the task will end. *Cognition, 197, April 2020*. Available at https://www.sciencedirect.com/science/article/abs/pii/S0010027720300081 (Accessed July 2024)

Kuzminykh, I., Yevdokymenko, M., Yeremenko, O. and Lemeshko, O., 2021. Increasing Teacher Competence in Cybersecurity Using the EU Security Frameworks. *International Journal of Modern Education & Computer Science*, *13*(6).

Open University, The (2020). *Qualification Learning Design Summary: R60 BSc (Hons) Cyber Security.* Available at: http://tinyurl.com/3tj5y9h4 (Accessed September 2023).

Open University, The (2022). *Staff Development Policy.* Available at: https://tinyurl.com/yn78zjz9 (Accessed March 2024).

Open University, The (2023). *Staff Fee Waiver Policy*. Available at: https://tinyurl.com/47es6u7x. (Accessed March 2024).

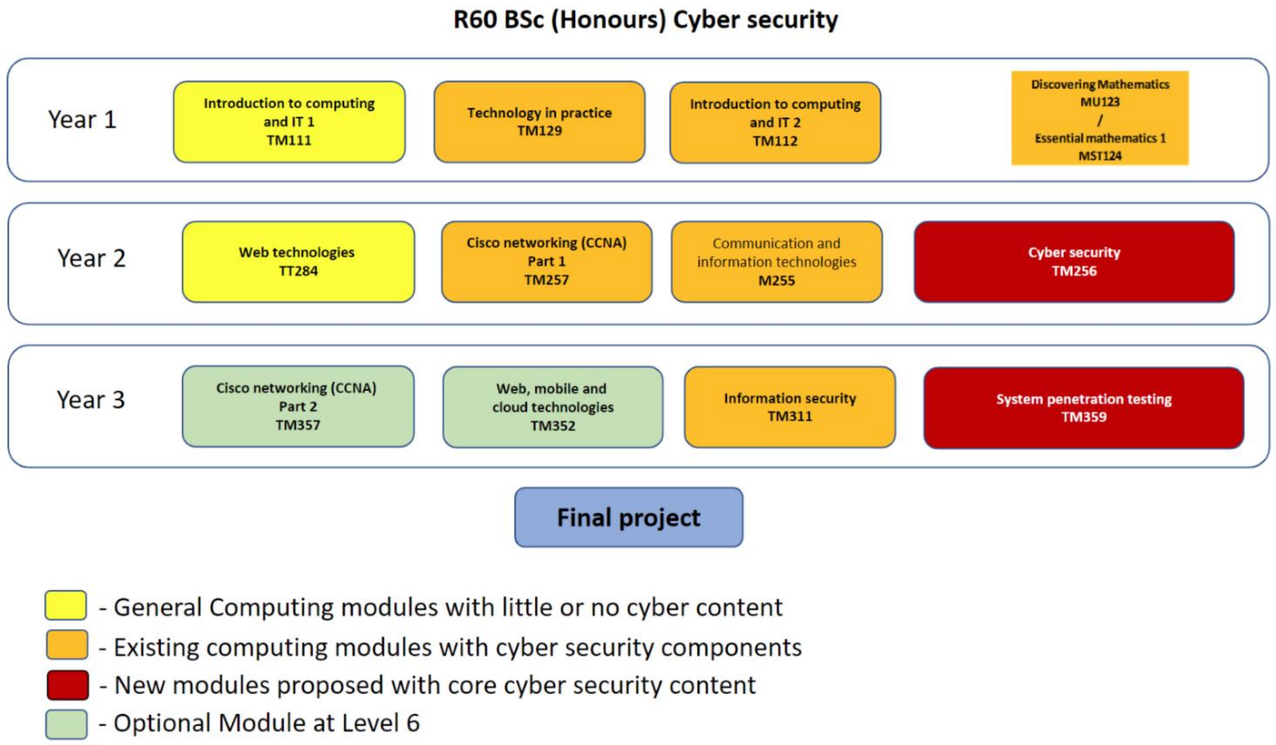
University approval processes

If your project required specific approval from university committees, please provide the appropriate information below. This is a necessary requirement for future publication of outputs from your project.

- SRPP/SSPP – Approval from the Student Research Project Panel/Staff Survey Project Panel was obtained according to the Open University's code of practice and procedures before embarking on this project. Application number: **407**
- Ethical review – An ethical review was obtained according to the Open University's code of practice and procedures before embarking on this project. Reference number HREC: **4946**
- Data Protection Impact Assessment/Compliance Check – A Data Protection Impact Assessment/Compliance Check was obtained according to the Open University's code of practice and procedures before embarking on this project. Data Protection registration number: **28-02-005**

Appendices

Appendix 1 BSc Cyber Security (R60) qualification map:



R60 BSc (Honours) Cyber security

Year 1

Introduction to computing and IT 1 TM111

Technology in practice TM129

Introduction to computing and IT 2 TM112

Discovering Mathematics MU123 / Essential mathematics 1 MST124

Year 2

Web technologies TT284

Cisco networking (CCNA) Part 1 TM257

Communication and information technologies M255

Cyber security TM256

Year 3

Cisco networking (CCNA) Part 2 TM357

Web, mobile and cloud technologies TM352

Information security TM311

System penetration testing TM359

Final project

🟨 - General Computing modules with little or no cyber content

🟧 - Existing computing modules with cyber security components

🟥 - New modules proposed with core cyber security content

🟩 - Optional Module at Level 6