Adult Cyber Skills Programme

Evaluation Report

Date of issue: 2021

Contents

Executive summary

The Department for Digital, Culture, Media & Sport (DCMS) commissioned QA to develop and deliver a virtual training offering, to inspire a diverse range of people interested in Cyber Security to pursue a career in the profession. This pilot programme will be used to inform future policy interventions.

As part of DCMS's wider work to increase the number of skilled people in the profession, and in particular to improve diversity and inclusion, QA developed a learning path that would support novices and individuals from different backgrounds, wanting a change of career or looking to step into Cyber security, to retrain and develop a portfolio of industry recognised skills and certifications.

The programme operated a 'no barriers to entry' approach to successfully train and upskill a diverse range of individuals in Cyber Security Fundamentals. The scope and intensive timescales for this project required QA to deliver all stages of the programme including attraction, recruitment, programme delivery, and evaluation within 12 weeks.

QA offered places to 200 learners with a flexible delivery schedule of four weekly timetable slots, enabling applicants with existing professional or personal commitments to attend training.

Each course consisted of 40 hours of online training, a combination of live delivery, knowledge checks, and immersive, self-paced labs. Trainers helped demystify the sector using real world experience with industry experts in the form of guest speakers, helping learners get to grips with the range of opportunity within the sector. A broad range of technical, non-technical roles, desired skills and day to day experiences were incorporated. On successful completion of the programme learners were eligible to sit the Association of Project Managers Group (APMG) and National Cyber Security Centre (NCSC) accredited exam: Foundation Certificate in Cyber Security (FCCS).

At the end of the programme…

- 95% of learners stated they were either satisfied or very satisfied with the learning experience overall.
- 92% of learners said they would be likely or very likely to recommend the training course to family and friends.
- 98% of learners were either satisfied or very satisfied with their course trainers.
- Qualitative data shows learners recognise they now have a deeper and more realistic understanding of the expectations of a role in cyber security.

- 94% of learners have at least some confidence to apply for an entry level role in Cyber Security on completion of the programme, compared to 53% before beginning the programme.
- 87% of learners were motivated/very motivated to continue to develop their cyber security skills, with a further 12% reporting some motivation to continue to develop these skills.
- 93% of learners are interested or very interested in IT/Cyber Security on completing the programme, compared to 72% before beginning the Adult Cyber Skills Programme.

Percentages representative of the 101 learners who completed the evaluation survey, out of a possible 143 learners who completed the programme.

- 75% of learners who sat the FCCS exam passed it first time, meaning that within 6 weeks of completing the course, 80 learners already have a foundational qualification in Cyber Security.

Figure true as of data available at 06.05.21, which tells us 106 out of the 143 learners who completed the programme, booked and sat the FCCS exam by 06.05.21. 80/106 passed first time. Learners will continue to sit or re-sit the exam post 06.05.21 which should increase the number of learners with a qualification.

Four aims were identified by DCMS for the pilot programme:

1. Promote cyber security as an exciting and recognised career choice.
2. Provide a quick and effective skills boost for successful candidates.
3. Encourage participants to seek out more training and/or explore further development opportunities in cyber security post-training.
4. Provide potential future employers with a clear breakdown of exactly what candidates will have obtained in terms of knowledge, skills, and any applicable experience.

QA designed the programme to meet these aims and has, within the accepted constraints, evaluated the efficiency and effectiveness of the programme to meet those aims.

1. 93% of learners left the programme declaring they were interested or very interested in IT/Cyber Security, an increase of 29% compared to pre-programme results. Almost half of learners (48%) had no confidence in applying for a role in Cyber Security before the programme. By the end of the programme, only 6% of learners report no confidence, demonstrating that this programme was successful at promoting Cyber Security as an exciting *and* recognised career *(see Appendices 4. 5).*

2. **Our evidence demonstrates that this was an effective knowledge and skills boost in the classroom, thereby laying strong foundations for learners to develop skills in real-world environments.** Our learners developed skill through immersive, self-paced labs in class which require practical application of knowledge. Confidence in knowledge goes a long way in enabling learners to turn knowledge into skill, and 87% of learners in the final evaluation declared confidence in all topics taught despite many being novices *(see Appendices 4.10)*.

3. **Motivation levels are maintained throughout the programme, with 99% of learners leaving the programme with motivation to continue to develop,** despite the programme becoming more demanding and exposing learners to the realities and complexities of Cyber Security. Post programme analysis builds on the evidence that **this aim was met** as the data shows that most **learners *have* pursued further development** *(See Appendices 4.4 & 4.14)*.

4. The mapping of content to existing and industry recognised standards, combined with learners possessing an industry recognised qualification and supporting statement, enables future employers to understand knowledge, skills, and experience obtained on this programme. **Whilst we met this aim, further work could be done on future programme design to better achieve this aim** *(See Appendices 4.13)*.

Three hypotheses were developed to evaluate if the pilot programme met the stated aims. QA sought to test these hypotheses through the collection of quantitative and qualitative data. The three hypotheses were:

1. People from diverse backgrounds and experience need to become aware of the opportunities that exist in cyber security.
2. Targeted and focussed training can sufficiently develop learners to progress to the next stage of capability development.
3. Industry will recruit people who have demonstrated an aptitude and motivation, and provide them with the experience needed for long term success.

We set out to draw data and produce an evaluation that would help DCMS understand implications for these three hypotheses. Below we outline what our evaluation can tell us about them.

1. **People from diverse backgrounds and experience need to become aware of the opportunities that exist in cyber security.**

   Our programme attracted a diverse candidate pool and inspired learners with a range of experiences and backgrounds to increase interest and awareness of the opportunity within the sector. We saw learners with little prior confidence, experience or understanding of the sector progress to become equipped with enough confidence, experience and

awareness to consider entering the profession and further their development in crucial cyber security skills *(see Appendices 4.4 onwards).*

This report gives evidence that it is possible, within a short amount of time, to take individuals with no or limited interest or awareness and transform their attitudes and understanding. As diverse groups of people "*can and do*" participate in, and benefit from, opportunities like this, we conclude that it remains important to continue efforts to raise collective awareness and opportunity for these groups.

2. Targeted and focussed training can sufficiently develop learners to progress to the next stage of capability development.

   99% of learners (who completed the survey) at the end of the programme expressed different levels of motivation to continue to develop after the programme. 138 out of a possible 143 learners are active on Cloud Academy *(description section 1.2*), where they are developing knowledge and skills in cyber related courses. *(See Appendices 4.4 & 4.14 for supporting data).* This evidence supports the hypothesis that individuals can *and will* go onto progress to the next stage of their capability development if they have access to targeted and focused training.

   Our multi-level training ensured learners had access to explore the range of opportunities that exist within the sector, via connections to industry experts, realistic challenges and focused subject matter that provided direct links to roles and opportunities. Combined with in house support and bespoke consultation opportunities, learners received continued support to understand how to maximise their opportunities beyond programme completion and importantly, develop the skills and confidence to pursue.

3. Industry will recruit people who have demonstrated an aptitude and motivation, and provide them with the experience needed for long term success.

   A longitudinal study is needed to meaningfully assess the implications for hypothesis 3, which sits outside the scope of this project.

We outline our impact and efficiency in meeting the programme aims and hypothesis in more detail in section *3.0 – Outcomes achieved by pilot*.

Based on the data available, QA's conclusion is that the four aims have been met to varying degrees, as outlined above. The hypotheses prove to be true with hypotheses 3 falling outside the scope of this project. The full report sets out the detail into how the aims were met and provides recommendations for DCMS to consider in the development of future policy and associated interventions.

In addition to the development and delivery of the training, the contract included an evaluation stage to support DCMS in learning from the pilot. QA proposed a theory of change model *(See 'Theory of change, page 9)* that was consistent with the Magenta Book to be used for the evaluation. This is the report based on that activity.

1.0 Introduction

1.1 Introduction to the Adult Cyber Skills Programme

The Cyber Launchpad programme is a pilot training programme for adults, designed to inspire potential career changers into cyber security roles at no direct cost to the student. The programme consisted of 3 levels of learning progression, increasing in difficulty and technical ability at each level. The Cyber Launchpad programme prepares participants to pursue a cyber-security career by covering the foundations of the digital world. The use of digital devices, networks, and data systems are explored in both a home and business context with an emphasis on how to implement effective security measures. As participants progress and build their knowledge at each level, they work as part of diverse teams on real-life challenges to explore the possible attack vectors and best practice security design considerations. The later stages of the programme provide an in-depth overview of key areas of cybersecurity including digital forensics, cryptography, open source intelligence, and penetration testing. On successful completion of the programme participants will have demonstrated an aptitude for cyber-security and will have a solid foundation to commence further accelerated training.

The Adult Cyber Skills Programme progression path is as follows:

Level 1: Cyber Connect

Identifying common cyber security threats, in the first line of cyber defences and networks. A focus on how these skills can be applied at home and throughout personal and school life, ensuring learners understand how to stay secure and help protect loved ones. Learners are introduced to the Cyber Security industry as a profession.

Level 2: Cyber Protect

Exploring the motivations for attack, understanding how to stay one step ahead in avoiding attacks and building knowledge on the functions of networks and their vulnerabilities. This is encompassed within the legislations surrounding cybercrimes and understanding the profiles of those who may carry out attacks. Learners are empowered to apply their knowledge beyond personal settings and consider how those skills can be applied in a business setting to solve current industry challenges. Learners develop their understanding of the realities and requirements of cyber security roles and are exposed to a variety of career avenues.

Level 3: Cyber Beyond

This course refines and deepens knowledge and practical application of skill, focusing on digital forensics, encryption technologies, open source intelligence, pen testing, and developing a deep knowledge of cybercrime recovery. The skills and confidence learners develop supports them to embark on a strong path into Cyber Security as an industry.

On completion of the programme learners gain knowledge of the foundations of cyber security. They can demonstrate that they have the aptitude for developing as a cyber security professional and understand the legal and ethical implications of technology applications in the real world. Upon completion, learners are able to take on early-career cyber roles or access further advanced training.

1.2 Pilot aims

To meet DCMS' policy aims, QA designed and delivered a programme based on these learner objectives:

- Increase the awareness and interest in cyber security as a profession.
  We set out to achieve this by supporting learners with limited or no prior technical experience to progress through a virtual learning programme, taught by industry experts and incorporating hands on labs, designed to inspire potential career changers.
- Generate the motivation of learners to go on to develop.
  We set out to achieve this by installing layers of progression opportunities, including post programme.
- Increase the confidence of learners to apply for a cyber security role.
  We set out to achieve this by providing a learning experience that connected learners to real world experience, industry experts, current opportunities, and helped them understand how their skills could translate into the sector.
- Help more people gain industry recognised qualifications.
  We set out to achieve this by equipping learners with the knowledge and support to access certification routes and bespoke learning paths on Cloud

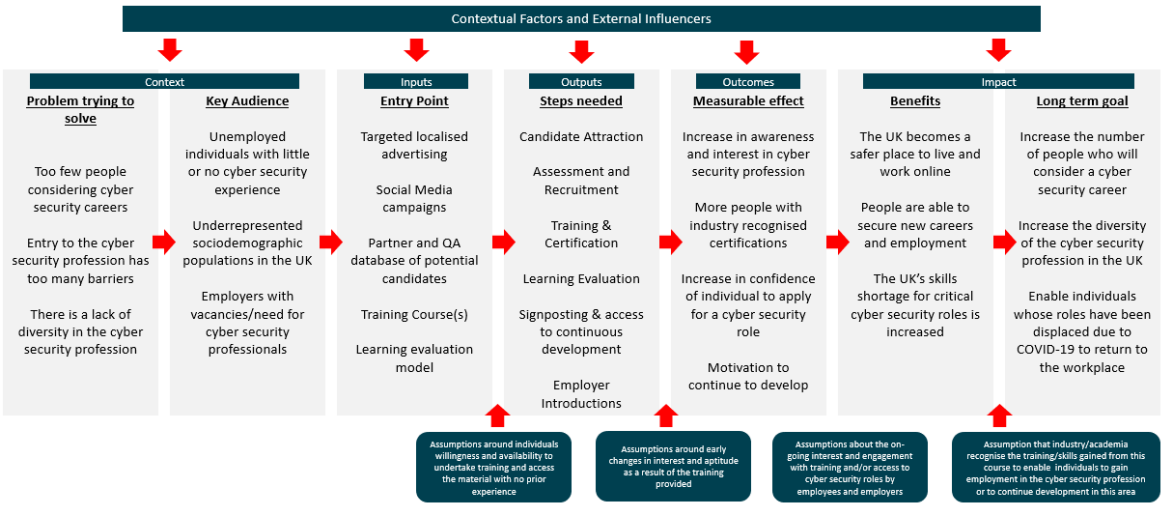
Academy at no direct cost to the learners. Cloud Academy is a virtual training platform providing over 10,000 hours of on-demand self-paced training to enable learners to continue to develop industry-recognised skills and gain certifications.

1.3 Evaluation scope and approach/methodology

Our evaluation approach focused upon measuring the pilot programme's effectiveness in meeting the aims laid out in section 1.1 above.

The evaluation was overseen by a Kirkpatrick Silver-level Learning Consultant, using the theory of change (see figure below) aligned to the model in the Magenta Book.

Theory of change



We focused on Levels 1 – 3 of the Kirkpatrick model to meet the evaluation criteria. Level 1 evaluation focused on the process evaluation, with Level 2 and 3 supporting the impact evaluation. Data and insights were collected with informed consent aligned to appropriate legislation using a variety of methods including heat maps, questionnaires, and rag status measures.

Due to length and structure of the programme being so short, the impact looked at in this evaluation focuses only on the short term and what can be realistically achieved within the timescales of the pilot programme.

The data and insights collected through this process inform the evaluation of the pilot programme and can support future policy interventions in this space.

The pilot programme key learning objectives are as listed in the executive summary, and we gathered the data and insights throughout the programme at 4 key touchpoints. *More information on these is detailed in the Pilot Programme Evaluation Data section 4.2.*

The data collected for this evaluation provides a point-in-time snapshot only.

1.4 Report structure

In the following sections we will break down each of the pilot programme aims in order to provide you with more detail of:

- The specific aim and any definition.
- The outcome - whether the aim has been achieved.
- Data points that connect to where it has been achieved.
- Key learnings and insights.
- Recommendations on a) future actions and b) things to change.

2.0 Candidate attraction and recruitment

2.1 Attracting diverse candidates

The findings of the National Cyber Security Centre and KPMG UK Joint report Decrypting Diversity: Diversity and Inclusion in Cyber Security, and IPOS MORI research into the UK Cyber Security Skills market highlight the lack of workforce diversity specifically around gender and those coming from lower socioeconomic backgrounds.

Attraction Aim

Attract diverse candidates from non-traditional talent pools.

Approach

- Remove barriers to programme entry, *(including setting a minimal entry level of knowledge, supporting learners onto programme even if lacked recommended equipment, flexible delivery times to accommodate variety of commitments such as childcare, Reasonable Adjustment provision).*
- Targeted marketing to reach key population groups, focusing on women and candidates from lower socio-economic groups (via QA.com campaign-specific landing page, QA existing database, digital marketing, social advertising, third party course advertising, and partnerships).
- Selection based on aptitude and motivation (aptitude measured by NCSC accreditor approved Questionmark assessment tool, motivation by letter of commitment).

Outcome

The data shows this aim was met in the following ways:

- 34% of learners were women *(compared to industry averages of 16% and NCSC Decrypting Diversity benchmark of 31%).*
- 28% of learners were from Ethnic Minority backgrounds *(compared to industry averages of 17%).*
- 61% of learners had no prior work experience in tech, showing a desire to break through into the sector.
- 21% of overall applications came from those who had been entitled to receive free school meals (compared to 17.3% of the student population in January 2020, according to gov.uk).

Key learnings and Insights:

Removing barriers to programme entry was a key enabler for increasing diversity. The data suggests that further work can be done to remove barriers to participation including:

- Continuing to offer courses at a variety of times to enable flexibility for learning, opening up the opportunity for learners who needed to balance this alongside other commitments such as childcare and part-time working.
- Supporting learners onto the course who didn't have the recommended equipment to ensure they did not miss out on the opportunity from lack of resource by allowing time to source equipment.
- Designating a base line level of knowledge and a key indicator of motivation as the only requirements for entry. This affords learners of low ability, who may not have had the opportunity to take up training before, the same opportunities as others.

Feedback from applicants showed that there is a reluctance to provide the sensitive data required for measuring diversity with many selecting the "prefer not to say" in data collection forms, a behaviour we also see across other programmes. We would recommend DCMS considers:

- Undertaking engagement activities that will boost applicant's confidence in the disclosure of sensitive data related to wider public outcomes. This could include the use of accompanying sentences such as "DCMS will use this data to improve the diversity of the profession". Similar statements are proving helpful in wider QA programmes.
- Demonstrate the benefit of providing diversity data for similar programmes to influence the future of the cyber security profession, by creating an action plan on increasing diversity within the profession which includes capturing diversity data and explaining how it will be used to drive change.

- Ensure that there is sufficient time in any further recruitment activity to explore alternative routes to capturing data and for better engagement with applicants to address any concerns they may have.

The January 2021 campaign ran for 10 days and attracted an applicant base where 46% were women and 60% from Ethnic Minority backgrounds. This demonstrates that there is a need and resulting appetite to generate awareness and interest in Cyber Security amongst diverse populations.

In the interest of meeting the set target of 200 learners, QA in agreement with DCMS, sourced applicants from alternative talent pools alongside the January campaign. This consisted of drawing on applicants for existing technical projects, selecting those who were unsuitable for them due to the technical requirement being greater than this programme.

This data suggests that:

- Extended time for targeted and focused marketing campaigns to generate enough applications to recruit from could increase diversity of upcoming talent in the sector.

Policy Considerations:

The contract required an accelerated attraction campaign which limited the time available to engage with and recruit the most diverse applicant pool possible. The data shows that the approach QA took was both efficient and effective in meeting the aim of attracting diverse candidates from non-traditional talent pools, but that this could be increased further by:

a) Future actions:

    - Starting candidate attraction campaigns earlier to increase the applicant pool.
    - Continue to use targeted approaches to recruit diverse groups – who may not be made aware of opportunities through standard recruitment channels.
    - Continue to offer a range of flexible delivery slots in future interventions.

b) Things to change:

    - A 2-part application process – to speed up the selection process and ensure that the demographic data is gathered effectively and in the right way. This could consist of a 'register your interest window' that is quicker to fill and requests upfront less personal information, followed by an email to complete an application.
    - Consider a support scheme to help learners who need it access recommended equipment (namely a second monitor). Whilst we do not have data that captures numbers affected, conversations

between learners and trainers on each cohort indicated that this had an impact at multiple stages in the programme. This experience tells us that supporting more people to access necessary equipment will raise the learning experience, attainment and ability to progress for future participants.

These interventions would enable a greater number of diverse individuals to more effectively engage and progress in their learning, increasing their chance of success and entering the industry.

3.0 Outcomes achieved by pilot

The Adult Cyber Skills Programme insights can be used to help inform future policy aims. In this section, we seek to explicate whether this programme met the policy aims, if so how, and identify recommendations to improve future interventions.

Aim: Promote cyber security as an exciting and recognised career choice.

Outcome:

By measuring interest at application and completion stage the data shows that the pilot programme was successful in increasing awareness and interest of cyber security as a career choice.

Key Data points:

- 72% of learners were either interested or very interested in IT and Cyber Security before attending the programme, rising to 96% after Connect, dropping to 91% in the middle after Protect, and rising to 93% at the end of Beyond.
- 94% of learners had at least *some* confidence to apply for an entry level role in Cyber Security by the end of the programme, with 35% reporting they were confident.

Key learnings and insights

The data suggests that the greatest increase in interest levels came after completion of Course 1; Connect. It is not unusual for interest to drop in the middle of a programme (Course 2; Protect) as people begin to understand the complexity of the topic and feel challenged by it. Interest increases again as confidence builds (Course 3, Beyond) and from wider experience we believe that for individuals who successfully move through this cycle there is the increased likelihood of sustained interest resulting in positive action. The data collected for this programme doesn't allow for this to be evaluated in this instance.

In the introductory course, learners are introduced to the concepts of Cyber Security and opportunities within the sector. It is designed to hook learners, and set a base level of knowledge which can then be built upon. We see that the course is highly effective in quickly transforming attitudes and raising the interest of learners where there was either none before or some before. It is natural that learners before this course were cautious in their interest levels as novices to the sector and that an opening course introducing them to the range of opportunities and the concepts they would learn more about fuelled this.

We expected to see a dip in interest levels at the end of Protect due to this course being significantly more challenging and technical, introducing some of the realities of working in the sector though immersive challenges that mimic real world scenarios. We can conclude that when working with novices, technical training can be off putting and dampen interest levels until their confidence and understanding grows through practice, support, and focused training.

The data shows that learners with higher technical ability develop, in general even more excitement about Cyber Security and can see themselves beginning a career within the industry even as the course becomes more technical. However, learners with less technical ability scored the same or lower, with qualitative data showing that the vast array of roles they were introduced to as possibilities could be overwhelming, resulting in them not knowing which path to go down. The increase in technical ability was also off-putting for some as learners wanted to know if all jobs required high level technical skills. We found highlighting the non-technical roles and training routes through Guest Speakers and Cloud Academy sessions helped promote Cyber Security as an exciting and recognised career choice to some of these learners.

Qualitative comments gathered during the evaluation process produced comments such as:

- ‘I really enjoyed the guest speakers as they brought a real-life aspect to how to apply this course.’
- ‘I found from one of the guest speakers that it is not just pen testing, there are a variety of roles within the cyber security, with a lot of different paths to take.’
- ‘The guest speakers really encouraged my spirit.’

Policy Considerations

- When considering Value for Money (economy, efficiency, and effectiveness) then it may be possible to achieve a significant increase in interest levels needed to help inspire potential career changers, through a shorter course that becomes the gateway for signposting other opportunities. Further testing of this approach would be required to validate this design.
- Sustained interest levels resulting in individuals accessing further training

and career opportunities may not be achieved with a purely Course 1 (Cyber Connect) approach. This would reduce the long-term effectiveness of the policy. The pilot does not enable this risk to be evaluated and therefore the recommendation is that it is tested in future phases of the programme. The risk could be further mitigated through engagement with potential employers who will be able to articulate the standard required to consider taking someone into an early career role.

- Interest levels are linked to an individual's confidence in the subject. In an accelerated delivery, all cohort participants are unlikely to develop at the same pace. Experience shows that where confidence doesn't increase with the subject complexity this becomes a barrier to engagement with the learning programme. Future programmes should consider options for extending the elapsed participation time to allow confidence to build ahead of increased subject complexity. The broad levels of prior experience of the pilot cohorts means there is not direct comparison to other programmes, however employer-led reskilling programmes consider learner-confidence in their design and will opt to extend the programme delivery over a longer time period for individuals with a lower starting knowledge. Recognising this is a potentially limiting factor in achieving the policy aims consideration should be given to how learner personalisation can be tested and then incorporated into future programmes.
- There is not a single-entry point or standard for all cyber security career roles and therefore consideration should be given to a programme design that recognises this and provides multiple entry and exit points. Future programmes may benefit from being designed against specific role outcomes (knowledge, skills, behaviours and attributes) so that the diverse pathways (entry, progression, and 'exit') are clearer to individuals and employers.
- A more comprehensive training solution that considers technical and non-technical dimensions may be more effective. The nature of roles in the Digital Age is placing a greater dependency on individuals being able to have knowledge and skills related to a technical domain but also engaging with different stakeholder groups to explore the role of technology for competitive advantage in business.

Aim: Provide a quick and effective skills boost for successful candidates.

Outcome:

The time constraints of this programme enabled us to test the confidence of learners and build the early stages of skills development through practical application.

Confidence in knowledge goes a long way in enabling learners to turn knowledge into skill through practical application and 87% of learners in the final evaluation declared confidence in all topics taught despite many being novices *(see Appendices 4.10)*.

The programme content requires learners to test and embed their knowledge through practical application in a virtual lab environment. Only once learners have successfully achieved this, solving challenges and tasks that mimic real-world scenarios, can they progress to the next level. Trainers monitored the progress of hands-on skills in the classroom setting.

Of the 143 learners who completed all stages of training, we can deduce that they have been effectively up-skilled by demonstrating practical application of knowledge to solve a range of challenges in class.

Beyond the classroom we have seen demonstrated in Cloud Academy learners practically applying knowledge to develop skill. This enables the platform to capture and measure skill *(See Appendices 4.14).* Without following learners on their journey post-programme, we cannot continue to measure skill outside of the classroom, and additional skills evaluation falls outside the scope of this project.

Key qualitative findings for this aim

- Most learners have moderate confidence in all topics taught despite many learners having no previous technical experience.
- Sample data shows that most learners have gained enough knowledge to be able to refine and advance skill sets via Cloud Academy. By providing learners with access to over 10,000 hours of self-paced digital training content QA has created the opportunity for lasting change in attitudes to learning to be embedded. This delivers real and significant value to the UK economy beyond the life of this programme.
- Learners who begin with lower capability in tech/Cyber Security entering the programme find it more challenging to develop their knowledge at the pace of the programme. Lower capability was determined by Questionmark scores and specialist trainers identifying learners who required additional support to progress.
- Learners found the more technical components on Course 2 more challenging and expressed interest in non-technical routes into Cyber.

Key learnings and insights

As of 06.05.21, 75% of learners who sat the Foundation Certificate in Cyber Security (FCCS) have passed the exam. This figure demonstrates that this course was an effective knowledge boost and will enable learners to continue to translate knowledge into skill once they have access to work-based environments or further development.

Scores in the areas of, confidence, motivation and interest, could have been higher, had lower ability learners been able to engage at a more suitable pace for their capability levels. *The data to support this can be found in section 4.0 of the Appendices, from 4.2 onwards.*

Learners gained an introduction to a wide range of industry related challenges, skills, and careers within Cyber Security, including legality and ethics. We recognise that some learners found the technical focus challenging and could have found the study of non-technical content a preferable option.

The majority of learners completed the programme with moderate confidence in all topic areas demonstrating that this was an effective intervention for all levels of capability. The increase in confidence and knowledge across the programme indicates that this programme was a successful solution to rapidly developing novices and potential career-changers *(see Appendices 4.10)*.

Policy Considerations

- Review the expected programme outcome for learners with lower starting capability against industry requirements (achieving the FCCS certification may not be realistic).
- Consider the programme scope to cover both technical and non-technical cyber security skills in greater breadth and depth with options to tailor delivery based on career destinations.
- Provide greater flexibility in programme delivery timescales to allow for learner confidence to increase ahead of subject complexity. This will additionally allow learners to embed their knowledge and reflect on what new opportunities they may now wish to explore.
- Incorporate the testing of skill at regular stages throughout a programme in future design. We recommend allowing more time to include potential employers and industry in the design phase.

Aim: Encourage participants to seek out more training and/or explore further development opportunities in cyber security post-training.

Evaluating the full impact of the pilot programme on this aim would require a longitudinal study which fell outside the scope of the delivery. We have provided some early indicators based on the evaluation we have carried out.

Outcome:

At the end of Beyond, 99% of learners who completed the course self-reported having at least some motivation to continue to explore further opportunities.

From this data and additional qualitative comments captured during the programme evaluation there is a strong indicator that learners have, and will continue to, explore further training and opportunities in Cyber security. This includes, but isn't limited to, making job applications, completing learning pathways on Cloud Academy and exploring apprenticeships, based on what some learners have shared to date.

Data points:

- 99% of learners (from 101 respondents in final survey) state they are very motivated, motivated or have some motivation to continue to develop their cyber security skills after completing the programme.
- Cloud Academy engagement rates show that 138 out of 143 learners who completed the programme, are already active on the platform, with a total of 216 learning pathways started and 86 completed *(true as of 16.04.21. More information can be found in the Appendices section 4.14).*
- Qualitative data shows learners appreciated the breadth of opportunities within cyber security presented (via content, guest speakers, Cloud Academy) but found it challenging working out the best one to pursue, particularly the non-technical routes.

Key learnings and insights

Providing a secure online environment within which to explore cyber security has reduced the reluctance to explore the profession. Building confidence through the programme to engage with the subject and identify role models helps people to believe they could belong in the industry. As a result, they are enthused to pursue new opportunities. The conclusion we draw from the data collected is that this style of intervention is successful at enabling a diverse range of participants to improve/increase their cyber security skills and knowledge. It also indicates that technical ability, prior experience or exposure are not required as a pre-requisite for those candidates looking to explore a career in this space.

Attitudes towards Cyber Security developed over the programme, with learners initially unaware of what opportunities were out there. As they began to realise the wealth of opportunities that exist in this space, they began the process of identifying which of these they would be best placed to pursue. Learners were keen to know more, using guest speaker visits, support resources and Cloud Academy to begin to narrow down suitable options. It was not in scope to capture this data however programme experience tells us that learners drew on these resources to identify their future options. Qualitative data backs up the idea that learners benefit from support, refining their future search options to match skill and interest. There is a need for awareness of the broad range of roles available but simultaneously they can become overwhelmed by the choice if there is no means of narrowing down options.

Presenting the full breadth of roles and capability levels within the cyber security profession, helps to address misconceptions about future career options. By addressing self-limiting belief through the programme design, it is possible to add further value and boost the individual's confidence to seek out

other opportunities.

In order to increase their chances of being successful in a competitive job market, 99% of learners *(from 101 respondents)* want to continue to develop their cyber security skills.

The Adult Cyber Skills Programme introduced learners to the vast array of sectors, roles and opportunities, and signposted learners onto further development through content, supporting resources, guest speakers, and Cloud Academy. The appetite for more post-programme bespoke consultation, indicates that an additional stage to this intervention, involving consultation and further support, would be taken up by learners.

A longitudinal study is needed to understand whether the current value add signposting in place for this programme is sufficient to encourage participants to seek further training. The value-add signposting consists of Cloud Academy support, including consultations and skills identification (for 6 months post programme), next steps newsletters and resources which share events, webinars, links etc, and finally optional subscription for further development opportunities.

Policy Considerations

- Recognising that there will be multiple entry, progression, and exit points from a longer-term programme there will be benefit in showing how the development of skills and knowledge at a specific point directly link to potential opportunities in cyber security. Learners will benefit from having the full learning pathway map to understand where they are currently developing and what the future training options may be. By showing the exit points from a learning intervention linked to potential career pathways will support individuals in managing their own development.
- Explore the benefits associated with providing an additional stage of the initial training, specifically focused on supporting individuals to enter the workplace including, but not limited to, soft-skills development, personal brand, and how to identify and apply for vacancies.
- Ensure there is the scope to signpost and support individuals in transitioning the new development opportunities at the conclusion of the initial intervention. This should be within the delivery scope of any future programme but DCMS may wish to consider providing a stand-alone solution from any specific learning intervention.
- DCMS should make provision for a Development Manager to nurture and develop post-programme interest and individual development. This role could be fulfilled by a future supplier if not undertaken by DCMS directly.

Aim: Provide potential future employers with a clear breakdown of exactly what candidates will have obtained in terms of knowledge, skills, and any applicable experience.

Outcome: The pilot programme meets this objective by providing individuals with access to an industry recognised qualification – *The Foundation Certificate in Cyber Security (FCCS).* This enables employers to identify knowledge against an established benchmark. The specific knowledge and skills learners gain is outlined in section 1.1 and learners are provided with a certificate and supporting paragraph (Appendices 4.13).

Course resources match content to roles and content is mapped to existing standards recognised by Industry, including the Cyber Security Body of Knowledge (CyBok).

As the course was designed to meet specific learning objectives associated with this aim, the individuals who successfully completed the course are able to clearly articulate the knowledge, skills, and experience they have acquired.

Data points

- 143 learners successfully completed the programme and 75% of learners who sat the FCCS exam, passed first time.
- 46% are either very confident or confident to apply for an entry level role, indicating confidence to articulate knowledge, skill, and experience to future employers.

Key learnings and insights

Learners who gain the FCCS certification will have an industry recognised qualification that can be benchmarked against other standards of education. This enables employers to quickly identify the level of skill and knowledge gained for each certification holder. The accreditation of Association of Project Managers Group (APMG) and National Cyber Security Centre (NCSC) as professional, awarding bodies leverages the recognition of this certificate to industry. The certificate demonstrates learners have a foundational knowledge in Cyber Security, which industry recognises. Learners can articulate additional experience and knowledge gained through the supporting paragraph provided (see appendices) or through additional courses undertaken through Cloud Academy.

The curriculum is also aligned to the DCMS sponsored Cyber Security Body of Knowledge (CyBoK) and existing educational frameworks which benchmark the skill and knowledge. The course content has been assessed as equivalent GCSE/A-Level. By mapping content to existing and recognised standards, employers gain clarity on the level of skill, knowledge, and experience completion of the programme provides.
This in turn enables a new pilot programme to be recognised amongst existing programmes, with the level and quality of the programme and its

graduates understood by employers despite being a new initiative.

Confidence levels *(see section 4.5 Confidence to apply for an entry level Cyber Security role)* on programme completion demonstrate that learners have enough understanding of the skills, knowledge, and experience gained to begin translating this into job applications for entry level careers.

Policy Recommendations

- The learning programme should be supported by resources which outline how the skills and knowledge are aligned to specific roles within the industry to support leaners in best identifying the routes for them to pursue. There would be benefit in linking to the (CyBoK) to support this.
- Future programmes could be better supported by increasing the employer networking opportunities and communicating to employers the benefits of the programme and involving them in the creation of the learning objectives.

3.1 Programme Evaluation Summary

This report has outlined how QA met the four policy aims stipulated by DCMS.

Drawing on qualitative and quantitative data we have shared learnings and insights with the intention of supporting DCMS to shape future policy in this space.

The insights gathered enabled us to suggest recommendations for DCMS to consider when developing future interventions to enable effective practice moving forwards.

Due to time constraints the data in this report is true as of the date of report submission or any dates attached to data. The rest of the report contains appendices where we share the supporting data for this report.

4.0 Appendices

4.1 Candidate attraction and recruitment data

Below is a summary of the data collected from the marketing and recruitment process. Where we have used the word '*applicants'* – this applies to all those who showed an interest in the programme. Where we have used the term '*booked* delegates or learners' – this relates to those who were successfully selected to take part in the pilot programme.

In the process of rounding percentages up and down to their nearest decimal place, not all pie chart percentages will amount to 100.

Candidate attraction

Gender

- The marketing campaign attracted a good mix of applicants, with 46% being women.
- Some of our top performing sources overall were our Facebook Ad, Coding Black Females, and CyberSecurity Jobsite.
- Imagery and language used was gender neutral which attracted more women.

Ethnicity

- 60% of applicants were from Ethnic Minority backgrounds, 38% White, and 2% Prefer Not to Say. 60% of applicants from Ethnic Minority backgrounds is significantly higher than the national average, where only 15% of the digital workforce are from Ethnic Minority backgrounds *(See Appendices 4.15)*.
- Targeted communications inviting ethnically diverse groups to apply for the opportunity yielded good results.
- Imagery and design assets were diverse and copy was taken through an augmented writing tool to remove any unconscious bias.

Employment Status

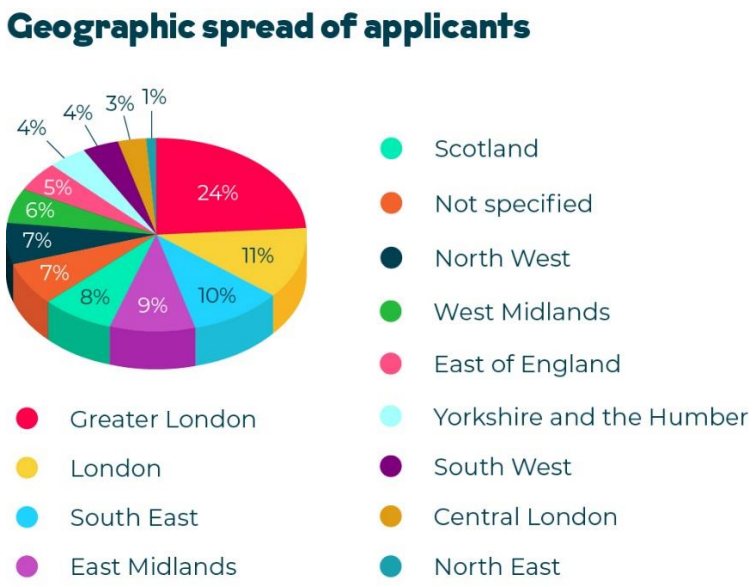
- We used targeted strategy and communications to ensure we had direct access to those that were unemployed and looking for their next opportunity.
- This came from using job centres, and location specific Facebook targeting where we focused on deprived areas.
- 52% of applicants were unemployed.

Socio-economic status

- 21% of overall applications received free school meals showing the appetite for roles in technology regardless of their socio-economic status.

Geographic spread

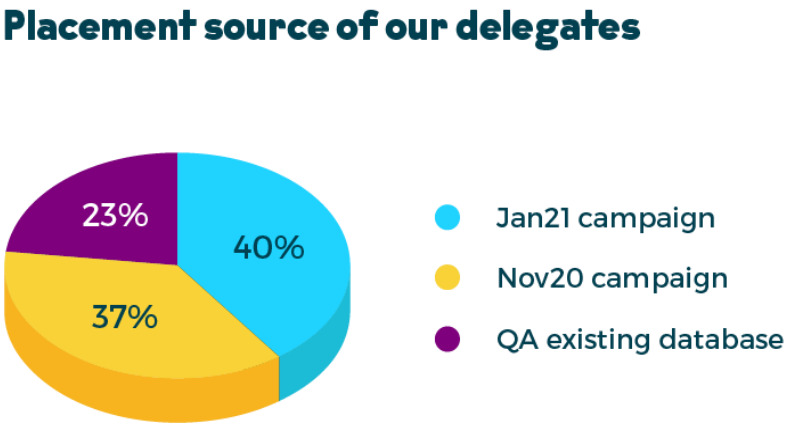
- Using partners who are engaging with communities across the country and publishing the course listings nationwide ensured a wide geographic reach.



Recruitment

Placement source

- More than **one in three learners came from the Jan21 campaign** – this is high considering the campaign was only live for 2 weeks.
- **The conversion rate of applicants from the Nov20 campaign was still strong, suggesting the script amends that we implemented were effective** and addressed the worries from the previous campaign.



Gender of booked learners

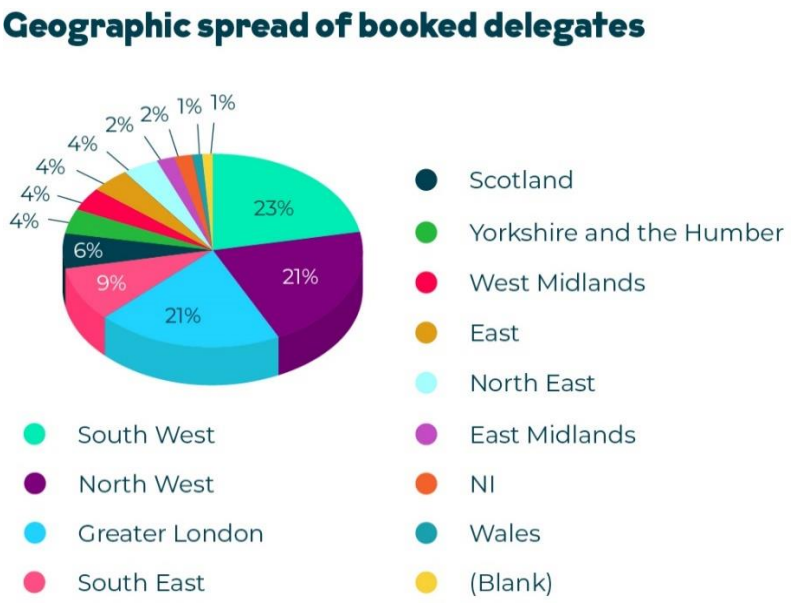
- **34%** of all learners successfully selected to take part in the programme were women.

Ethnicity of booked learners

- 28% of booked learners were from Ethnic Minority backgrounds - higher than the national average where only 15% of the digital workforce are from Ethnic Minority backgrounds *(see Appendices 4.15)*.

Geographic spread

- Learners booked on represent a good geographic spread across the UK.
- The South West, North West, and Greater London provided the highest number of learners.



Prior experience and education

- 61% of applicants had no prior experience in tech, showing a passion and desire to break-through into the sector regardless of their past work experience – highlighting the inclusive nature of the campaign which had little to no barriers to entry.

Conclusions from evaluation data gathered across four touchpoints

The data shows that the learner demographic for this programme represented a diverse range of individuals with a varied amount of experience from a number of different backgrounds and geographical locations.

It is our belief that the learner pool for this pilot programme met the requirements highlighted as desirable by DCMS in the scoping phase and in line with industry averages provided by DCMS (see Appendices 4.15).

4.2 Pilot programme evaluation data (taken from four touchpoints)

In this section we share the data collected at the start and end of the complete learning journey, plus some key milestone data gathered between touchpoints.

At the very start, then following completion of each course, learners were asked to complete a questionnaire using MS Teams forms. Reponses were collated once all 8 cohorts had completed each course in order to maximise the number of respondents included. The questions offered a combination of quantitative and qualitative data to support the hypotheses discussed in the introduction of this report and to fulfil the evaluation criteria set out at the scoping phase of the programme.

4.3 Interest in IT/Cyber Security

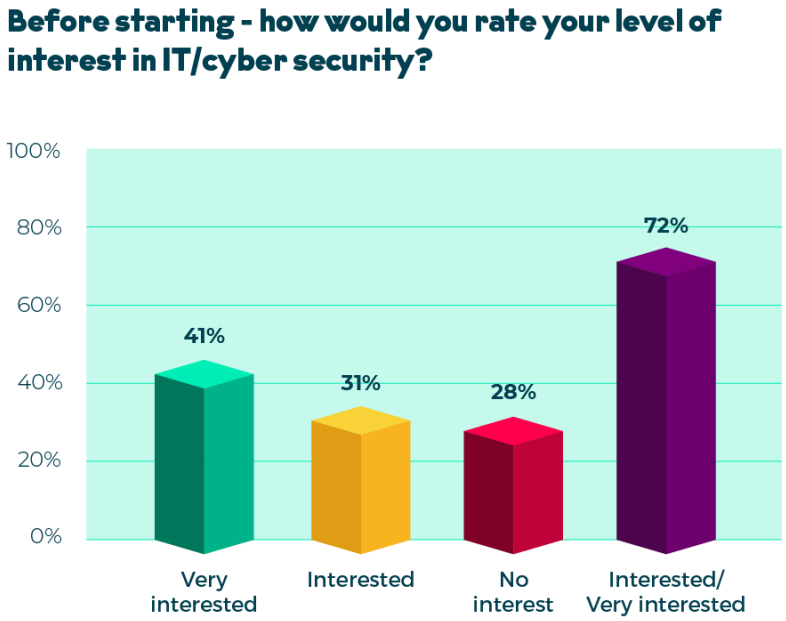
At the start of the programme

On day one of their first course and before any learning had taken place, learners were asked 'before starting your training – how would you rate your level of interest in IT/Cyber Security?'.

- 72% of learners were either interested or very interested in IT and Cyber Security. Some of the recurring themes in their reasons included:
    - Wanting to up-skill and learn more about cyber security
    - Wanting to re-skill and do something different/change of career
    - Had researched the topic and were interested to learn more
    - Had always loved computers and technology
    - High number of job opportunities on the market in this field
    - Interested in the 'ethical' and 'preventative' nature of this area

A number of respondents indicated a willingness to learn and develop, despite knowing very little about cyber security. This is reflected in some of the data captured further in this section.

- A total of 28% of people reported 'no interest'. Reasons for this varied, including:
    - A limited level of knowledge and therefore had not previously shown an interest
    - Those who didn't believe they'd be able to learn the technical aspects
    - Those who appreciate the importance of it but had not considered it in terms of a future career



Total number of respondents: 175

Decimal places have been removed for data cleanliness – those at .5% or above are rounded up; those below .5% rounded down.

During the programme

After just 2 weeks of training, there was a large rise in interest levels, with 23% more learners reporting being interested or very interested in IT/Cyber Security.

We also saw that 24% less learners reported having no interest. Only 6 out of 137 learners stated they had no interest after the first 2 weeks of training, compared with 49 out of 175 at the start of the programme.

Towards the middle of the programme, interest levels dropped by 5% in the very interested/interested scores (whilst remaining 19% higher than at the start of the programme). We also saw an increase of 5% in learners who stated they had no interest in IT/Cyber Security.

Comments gathered through qualitative feedback shows that as the programme moves fairly rapidly into the more technical elements of cyber security topics and concepts, we see learners who are less technically capable start to display a level of uncertainty around their skills and knowledge. The practical hands on labs and activities challenge them to put their skills and knowledge to the test and this can be daunting for some.

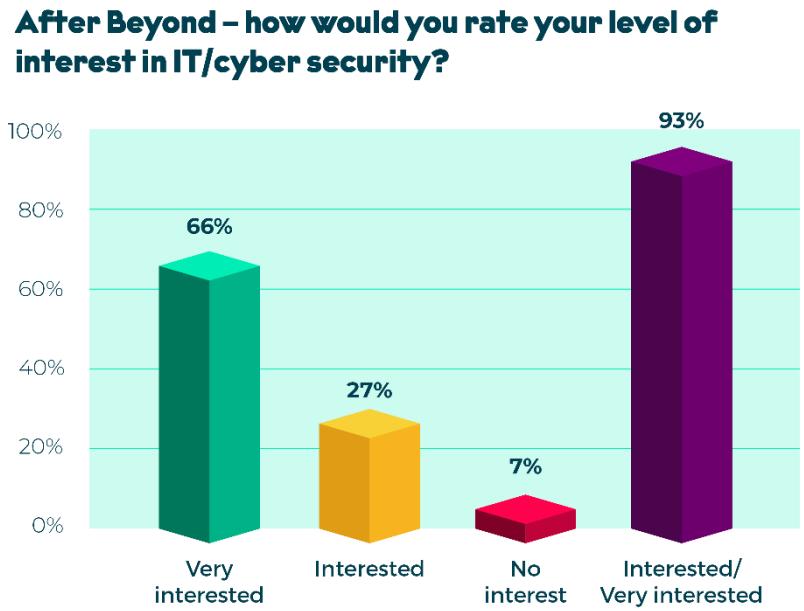
In contrast, it also introduces learners to the variety of roles available in this field of work, both technical and non-technical – so for some there was the realisation that they may be able to consider other opportunities in the cyber security world of work that did not necessarily require very technical skills.

Whilst for some it started to become far more technical than they'd anticipated, for others the increase in technical content was interesting and challenging and encouraged them to want to learn more.

At programme completion

Following completion of all three courses and reaching the end of the programme:

- Interest levels have remained high - despite Beyond taking skills to a more technical level.
- The proportion of those saying they were interested or very interested in IT/Cyber Security since the start of the programme increased by 21%.
- Those very interested increased by 25% since the start of training – with this increase happening after the first two weeks *(after Connect)* then remaining at a similar level throughout the remainder of the programme.
- 7% of learners (7 learners) say they have no interest in IT/Cyber Security – with the key reasons stated being linked to self-awareness around lower capability levels mixed with an acceptance for some that having tried, it's not for them.



Total number of respondents: 101

Decimal places have been removed for data cleanliness – those at .5% or above are rounded up; those below .5% rounded down.

A selection of the comments in relation to the levels of interest shown at programme completion can be seen below.

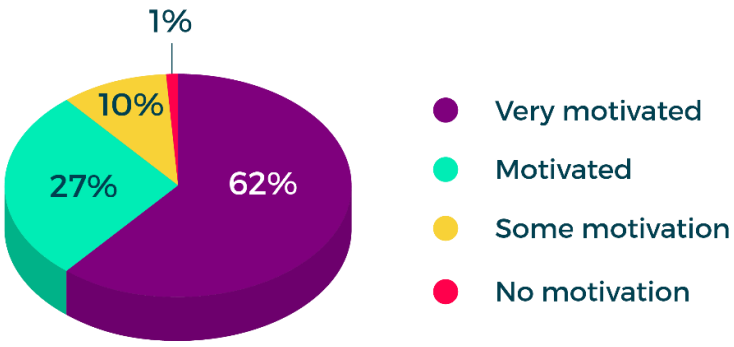
These were a complete mixture of those who were eager to continue and pursue a career in cyber security, versus those who were more cautious and wanted to continue to learn and develop to improve their knowledge and skills before becoming more confident. Some felt it was a vast area that would require more dedicated time in order to successfully get into.

4.4 Motivation to continue to develop

At the start of the programme

Before beginning any training, the data shows us that 62% of learners are very motivated to continue their development in cyber skills and 28% are motivated. 10% of learners had some motivation with only 1% showing no motivation at the very start. This equated to only 1 learner, who did not offer any additional explanation for reporting no motivation at the start.

Before starting – how motivated are you to continue your development in cyber skills?



Total number of respondents: 175

Decimal places have been removed for data cleanliness – those at .5% or above are rounded up; those below .5% rounded down.

During the programme

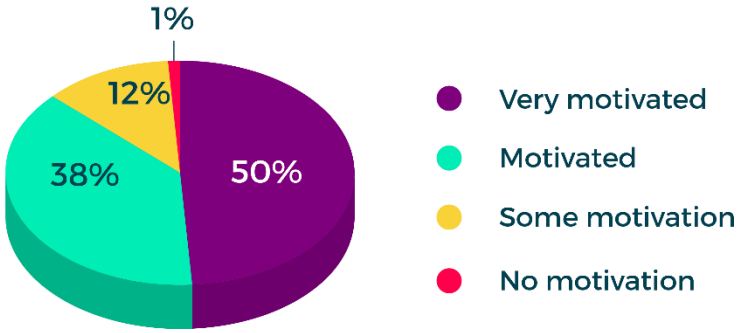
The numbers of learners who want to continue developing skills, remain at a consistent level throughout all three courses, showing that those attracted during the launch remain motivated throughout the first and second course of the programme.

At programme completion

The numbers of learners who want to continue developing skills remains high, with those very motivated having dropped a little by 12% since the start - and those motivated increasing by 11% since the start of training.

Those with some motivation have risen slightly by 2% - with just 1 learner (1%) who states they are not motivated to continue. No reason was offered for this – although this particular learner's scores have remained low throughout the entire programme.

After Beyond – how motivated are you to continue your development in cyber skills?



Total number of respondents: 101

Decimal places have been removed for data cleanliness – those at .5% or above are rounded up; those below .5% rounded down.

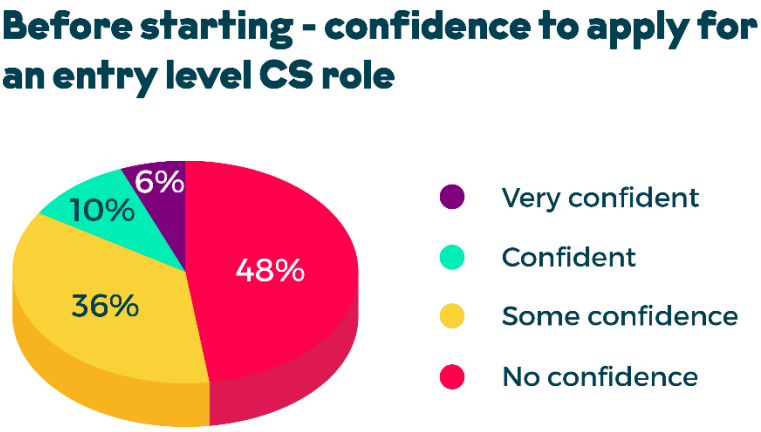
4.5 Confidence to apply for an entry level Cyber Security role

At the start of the programme

At the very start of their learning journey, before commencing any training on the programme, almost half of the learners (48%) reported no confidence in applying for an entry level CS role.

Of those that showed any level of confidence, they demonstrated a mixture of previous experience and capability with some having no experience at all and others having some experience.

There was no strong data at this stage to suggest that confidence levels and capability were necessarily linked. Some who had no knowledge at all of cyber security were confident to pursue a career in this field.



Total number of respondents: 175

Decimal places have been removed for data cleanliness – those at .5% or above are rounded up; those below .5% rounded down.

During the programme

As learners progressed through the first Connect course there was a significant shift in the levels of confidence with many learners moving from a place of no confidence to some confidence. At the end of the first two weeks:

- 12% are very confident to apply for an entry level role CS role, 6% more than pre-programme.
- 20% are confident to apply for an entry level CS role, 10% more than pre-programme.
- 56% have some confidence to apply for an entry level CS role, 20% more than pre-programme.
- 11% show no confidence in applying for an entry level CS role, 37% less than pre-programme.

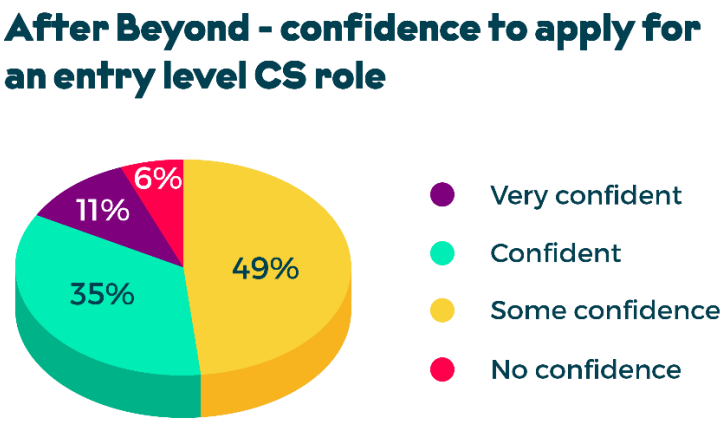
Whilst there was less of a significant shift towards the middle of the programme, this is expected as the course content moves from a very individual focus on cyber security to more of a business and organisation focus – becoming more challenging and technical as it progresses.

Additional expectation on the learners at this stage of the programme comes in the form of the Learning on Demand and additional practical activities that they are required to complete in order to progress and develop their skills and knowledge. Some will naturally find this daunting and uncomfortable and it may cause them to reconsider their options.

At programme completion

On completion of the Beyond course and reaching the end of the programme, 94% of learners have some level of confidence in applying for an entry level role in cyber security – a big improvement from almost half (48%) at the start showing no confidence at all. At the end of the programme, there are

6 learners, from 101 respondents, who say they are not confident to apply for an entry level CS role.



Total number of respondents: 101

Decimal places have been removed for data cleanliness – those at .5% or above are rounded up; those below .5% rounded down.

4.6 Attitude towards Cyber Security

At the start of the programme

Before commencing any training at all, learners were asked to describe their 'attitude towards Cyber Security'. Below is a collection of the comments that were received in answer to this question.

Initial comments showed that all those who had been recruited into the programme had a very positive attitude towards cyber at the start, were keen

and willing to learn more in order to deepen their understanding and some showed recognition of the importance of this topic in our society today.

During the programme

On completion of the Connect and Protect courses, learners were asked:

'Before starting your training, you were asked to describe your attitude towards Cyber Security – what if anything has changed now as a result of attending the Connect and Protect courses?'

From 137 respondents in total for Connect, 36 learners (26%) said their attitude had not changed – in that it remained the same as it was at the start at the programme.

Many respondents gave positive comments in answer to the question, including:

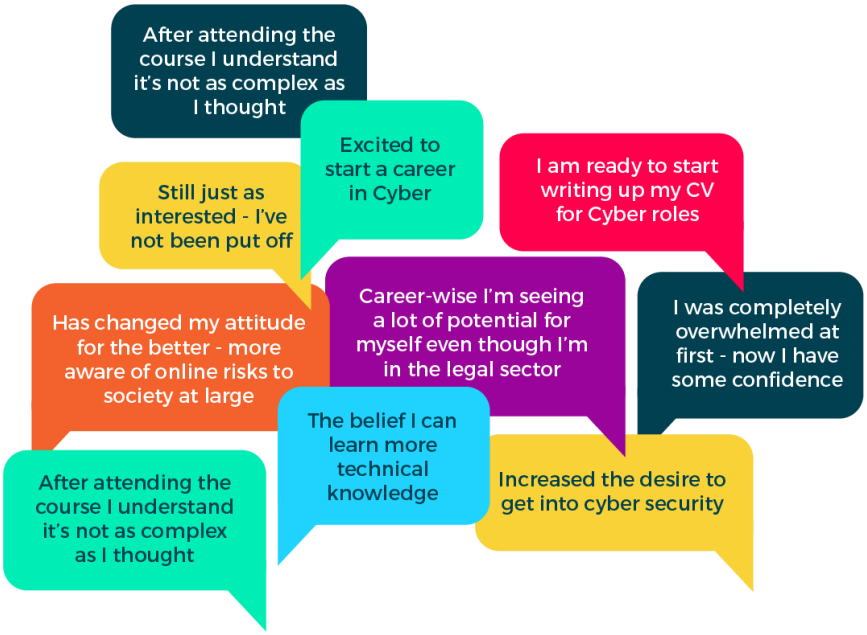
- Being even more interested and passionate than before.
- Wanting to learn and know more.
- Having had their eyes opened to the world of cyber security.
- Having more knowledge as a result of what they'd learnt already.
- An increased desire to get into cyber security as a career.
- Being more aware of the dangers – and subsequent need for cyber security.

Others reported concerns such as:

- Being more aware – but not fully comfortable.
- Now aware of how much I really don't know.
- Too much to learn at the beginning – gradually getting better though.

Below are some of the other comments gathered in response.

Below is a snapshot from the responses captured immediately following completion of the Protect course, towards the middle of the programme.



This time the data shows us a new direction for some learners in their thinking. Many have moved from an awareness of their own personal security and safety online – to now thinking about the possibility of a future career in cyber security and the different roles available in that field of work.

We also see differing levels of ability having an impact – for example those who are more technically capable talk positively about the more technical

roles in cyber – or show more confidence in the learning content.

Those with less capability show some hesitation – using terms like 'it's a scary new world'. There are still high levels of interest among this set of learners – and still the motivation to develop – just an air of caution around whether it's a future for them or not.

At programme completion

Following completion of the Beyond course, learners were again asked the same question. Themes from the responses received again tells us that while interest levels continue to be high and knowledge and skills have further developed, people's attitude towards cyber security is still very positive, even where capability levels may be lower.

4.7 Understanding of the expectations of a Cyber Security role

At the start of the programme

Before commencing any training, learners were asked to tell us what their expectations of a cyber security role were. A selection of the responses is shown in the table below.

To help protect the public against malicious attacks online	To test and implement cyber security measures for businesses
Protecting data and networks from unwanted visitors	Monitoring networks for breaches or attacks
Managing risks and assessing how secure a network is and working to make it more secure	That it is a necessary role that must be performed by highly trained individuals
That it's an important and responsible role	To prevent cyber attacks and attack ethically
I have limited knowledge of what it involves on a day to day basis	To prevent security issues for companies
Requires hard work, constant learning and adapting to new threats	To guard and secure networks; to identify risks and threats and defend against attacks
That roles can be varied and encompass different areas	I'm not sure/virtually none

Responses from a total of 137 learners at the start of the programme show a mixed level of understanding. Some are very knowledgeable about the role that cyber security plays in our environment.

Others have some knowledge which is limited and some freely admit to having very little knowledge at all or have said they have virtually no

knowledge or understanding and are willing to learn.

During the programme

Following completion of the Connect course, learners were asked the same question again – this time 'what has changed' with regard to your understanding of a cyber security role since completing the Connect course.

From the 137 responses received, the data showed that learners are starting to gain a clearer understanding of cyber security in terms of the skills required to pursue a role in this field. Learners recognise there are varied roles and responsibilities within the cyber security profession and some acknowledged they still had some way to go in order to gain the knowledge and skills required.

The table below shows a selection of these comments:

My understanding changed dramatically - now I am far more aware of the skills needed to pursue a role in the industry and it will help me draft a realistic plan to build it and land a new position	I thought it was difficult and complicated but after finishing the course I have a good foundation to build on and hopefully work within IT and Cyber Security
There are different sides of cyber security - more varied roles to choose from	It seems as technical as ever
Crucial that flexibility and adaptability is part of the skills set of a cyber security professional	There are aspects of the job that I did not know about
Learned how much broader it is - looking forward to finding out more and learning to specialise from there	Better understanding of some of the responsibilities
Considerably - the scale of the challenge is clearer	Feel like I need to be even more knowledgeable to get to the bottom of this
It's been demystified a bit - some more knowledge needed to understanding the requirements for a cyber security role	I can see the creative approach this field takes when it comes to finding vulnerabilities
Made me more interested after finding out just how poor some networks can be	Been an eye opener - very intriguing and not your run of the mill job
You use more tools than I thought - it's not all code code code!	

Following completion of the Protect course, where learners were asked the same question again, from a total of 93 responses we saw an increased level of awareness and understanding around the number of varied roles that exist in the field of cyber security.

Whilst some were still of the mindset that this is a very technical profession, others were more open to the possibility that there were other roles in cyber security that didn't require as much technical expertise or knowledge.

Some of the comments are summarised in the table below:

Massively - it has shown a clear divergence in paths for technical and non-technical roles, so has given me some impetus to find out more about the non-technical roles.	There is no sentiment, I see cyber security role as duty to protect humanity considering the multi dimensional ways attacks are being carried out and the motives behind the attacks.
My understanding has developed a lot in terms of how business need to consider Cyber Security. I was only marginally aware of this before starting the course.	I find a role in cyber security more interesting now because the knowledge gained form this course has been an eye opener
I knew it would be challenging as I have no IT experience.	It seems a lot more attainable
There is a huge industry out there to explore	It is pretty much as I expected but it goes a bit deeper than I had originally thought.
I've been able to narrow down where I may want to work i.e. not	I respect it a lot more.
Requires an up to date knowledge of networking and increasingly cloud infrastructure.	I now know what field to go into.
Really learn to know about lots of things in computer security	You have to think outside the box
A lot. Now I understand that cyber security doesn't just need technical skills, but a good mix of soft skills as well. And that a lot of roles don't need a lot of technical skills	

After Beyond

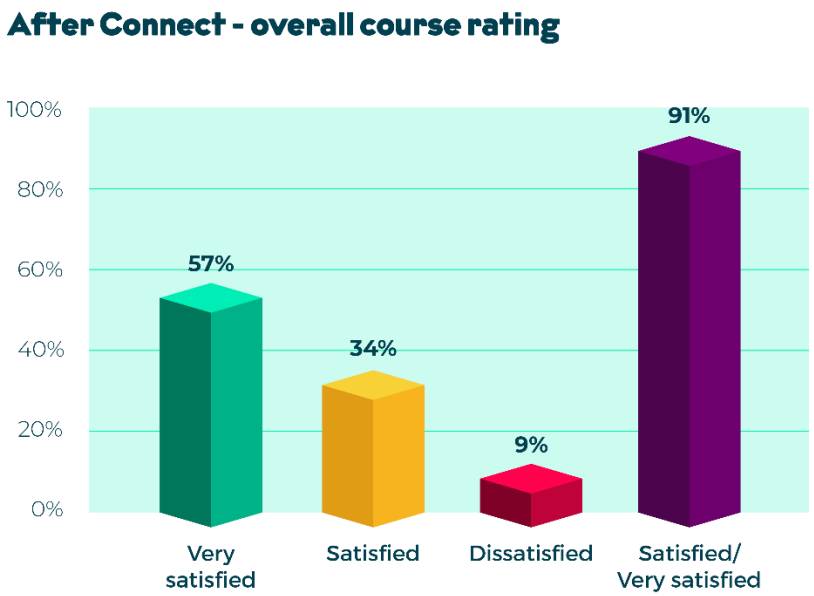
Following completion of the Beyond course where learners were again asked the same question, the 101 total number of responses show that learners recognise they now have a deeper and more realistic understanding of the expectations of a role in cyber security.

It has changed immensely	There is so much to a cyber role and it doesn't have to be technical
By background knowledge has grown	I know how I need to develop further
Yes – it's more interesting!	I now realise how much you need to learn on the job – it needs an apprenticeship or relevant experience
It goes much deeper than I expected it to	I initially felt that I had to know it all – I know realise it's a role of constant learning
My understanding of the wide variety of areas to cyber security has changed.	I have a deeper understanding now
It's a more realistic understanding	My understanding has evolved over the course of the programme
I know there is more involved – and multiple jobs within it too	I know now what I need to learn to be successful

4.8 Pilot programme ratings overall

Overall course ratings

After Connect



Total number of respondents: 137

Decimal places have been removed for data cleanliness – those at .5% or above are rounded up; those below .5% rounded down.

At the end of the first training course, Connect, around 91% of learners were either satisfied or very satisfied with the course overall.

13 learners (9%) of learners reported levels of dissatisfaction with the course overall, with the reasons for the dissatisfaction including:

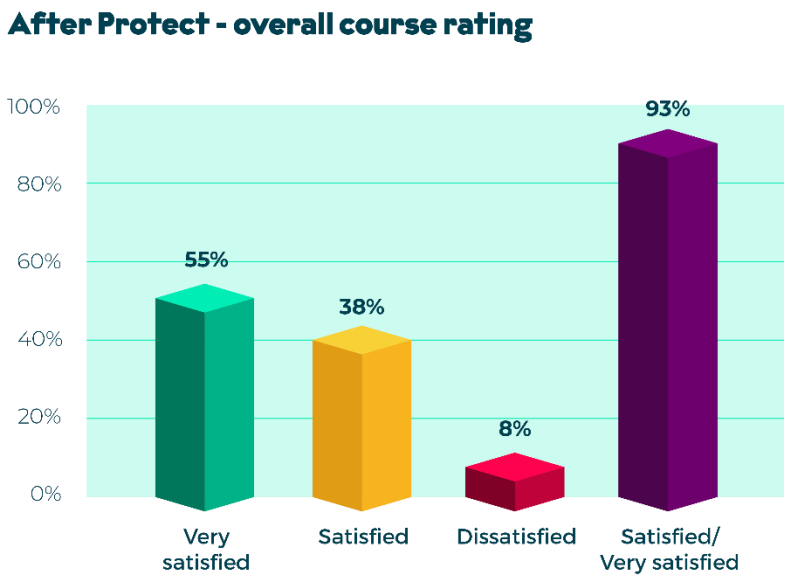
- The course feeling rushed – lots to cover in a short amount of time.
- The learning requiring a higher level of experience.
- Needed to do a lot of study in own time.

After Protect

At the end of the Protect course, 93% of learners were either satisfied or very satisfied with the course overall, with 8% showing a level of dissatisfaction.

Reasons for the dissatisfaction at this stage were themed around:

- Lower levels of capability making it harder.
- Lack of time spent on hands on practical elements.



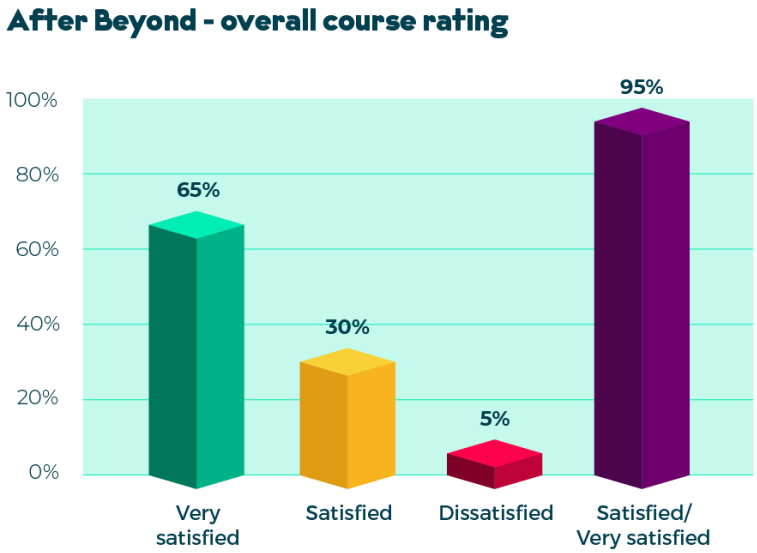
Total number of respondents: 93

Decimal places have been removed for data cleanliness – those at .5% or above are rounded up; those below .5% rounded down.

After Beyond

At the end of the Beyond course, 95% of learners stated they were either satisfied or very satisfied with the learning overall.

5 learners showed levels of dissatisfaction with an average score of 4.6 out of a possible 10. Reasons of dissatisfaction included there being a lot to take in and some feeling a lot less experienced than others in the cohort.



Total number of respondents: 101

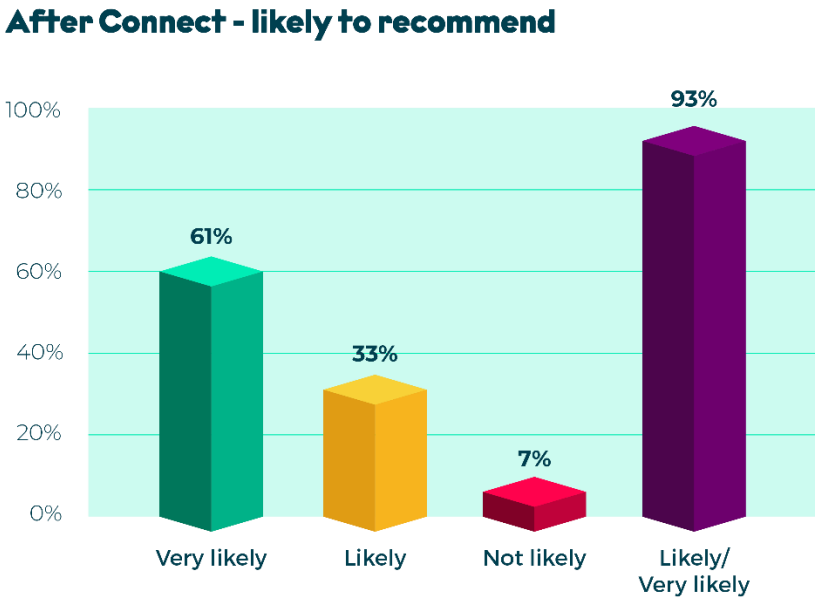
Decimal places have been removed for data cleanliness – those at .5% or above are rounded up; those below .5% rounded down.

Likely to recommend ratings

After Connect

At the end of the Connect course, 93% of learners said they would be likely or very likely to recommend the training course to family and friends. Only 7% stated they were not likely to recommend the training with reasons that included:

- You need solid IT knowledge.
- It's quite a steep learning curve.
- Needs more information on vulnerability management.



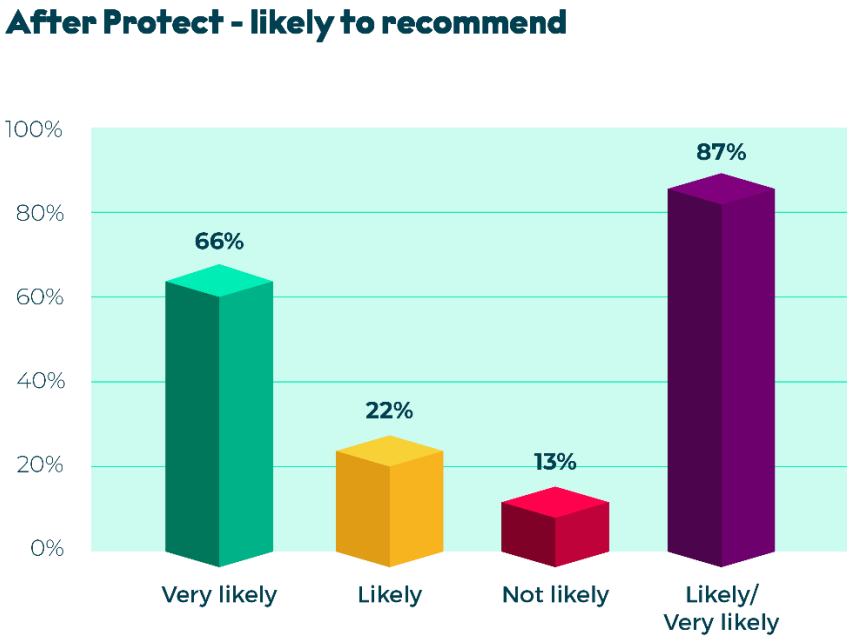
Total number of respondents: 137

Decimal places have been removed for data cleanliness – those at .5% or above are rounded up; those below .5% rounded down.

After Protect

Following the Protect training, 87% of learners said they were likely or very likely to recommend the course to family and friends. This time 13% said they were not likely to do so and the reasons for this included:

- Course requires IT knowledge and is challenging.
- Good broad introduction to key concepts but quite time intensive.
- Perfect if you already have a little experience.



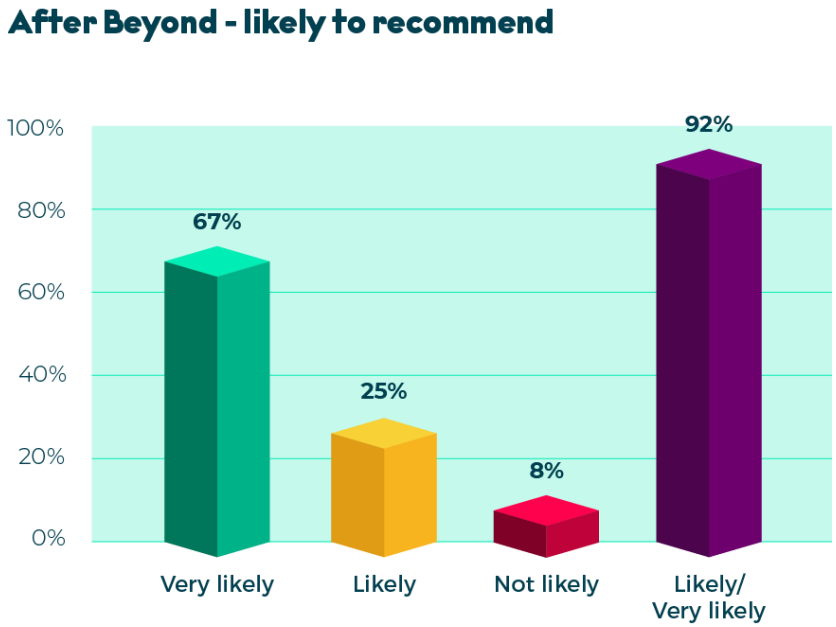
Total number of respondents: 93

Decimal places have been removed for data cleanliness – those at .5% or above are rounded up; those below .5% rounded down.

After Beyond

At the end of the Beyond course, 92% of learners said they would be likely or very likely to recommend the training course to family and friends. 8% stated they were not likely to recommend the training with reasons that included:

- It's a big challenge and commitment to make if you're not from an IT background.
- Not likely, based on how much has been learned and understood.
- There was an imbalance of skills sets which made it harder for those less experienced.



Total number of respondents: 101

Decimal places have been removed for data cleanliness – those at .5% or above are rounded up; those below .5% rounded down.

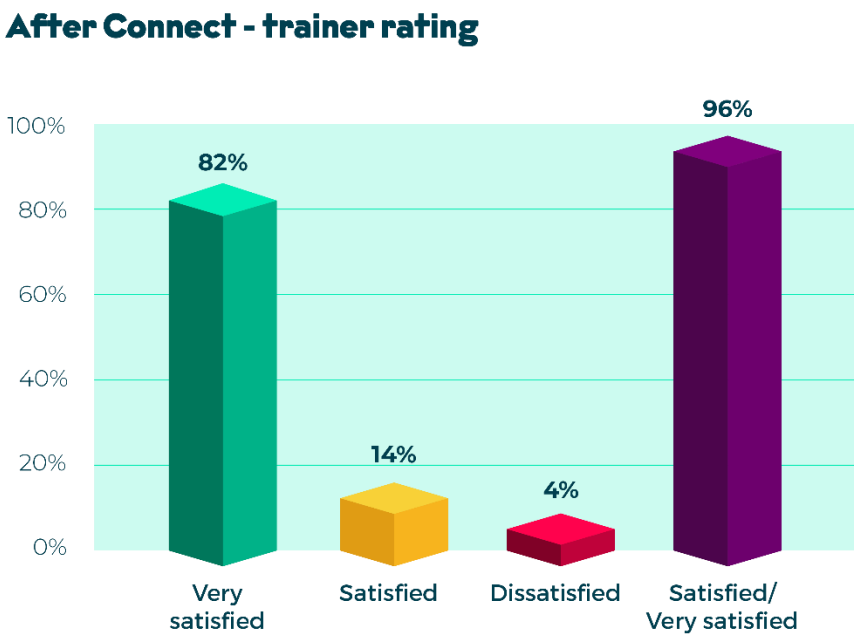
4.9 Trainer feedback

After Connect

At the end of the Connect course, 96% of learners were either satisfied or very satisfied with their trainers, sharing positive comments and feedback in support of their scores.

4% of learners reported levels of dissatisfaction, with reasons including:

- Allow more dialogue between learners.
- No daily timetable.
- More consideration needed of learner levels of knowledge/understanding.



Total number of respondents: 137

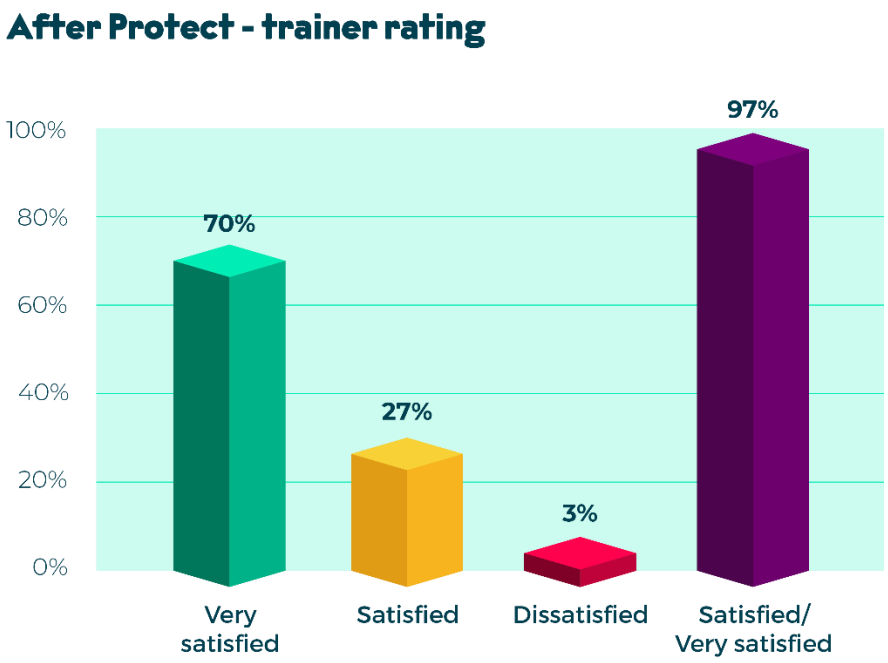
Decimal places have been removed for data cleanliness – those at .5% or above are rounded up; those below .5% rounded down.

After Protect

At the end of the Protect course, 97% of learners were either satisfied or very satisfied with the trainers.

3% of learners were dissatisfied, with reasons including:

- A lot of trainer talk time.
- Could have defined purpose of the activities more clearly.

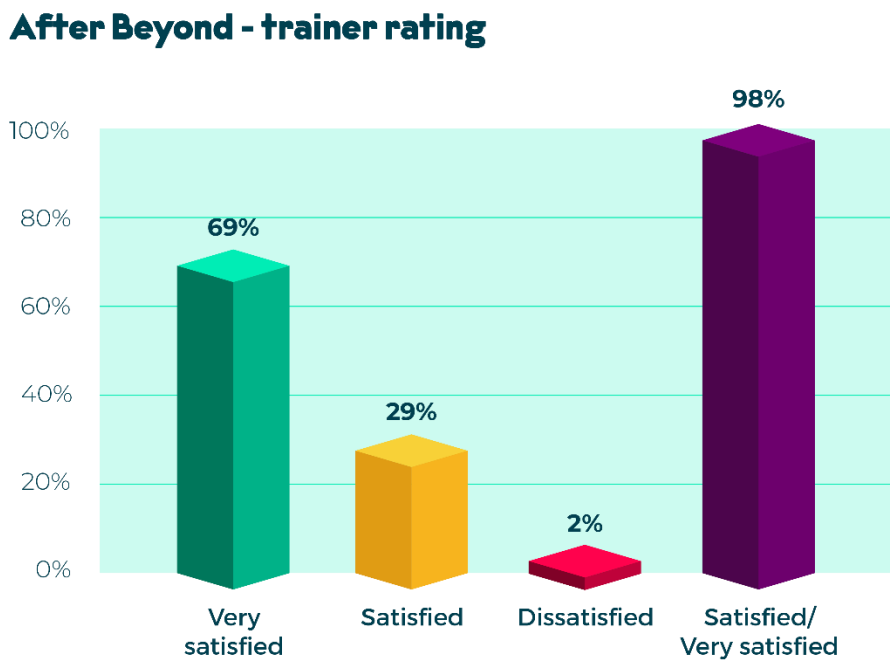


Total number of respondents: 93

Decimal places have been removed for data cleanliness – those at .5% or above are rounded up; those below .5% rounded down.

After Beyond

At the end of the Beyond training, 98% of learners were either satisfied or very satisfied with their course trainers. 2% of learners (2 learners) stated dissatisfaction – one scored a 6 and said they were 'fine' – the other said they'd had more engaging trainers in previous sessions and so were comparing with these and scored 4.



Total number of respondents: 101

Decimal places have been removed for data cleanliness – those at .5% or above are rounded up; those below .5% rounded down.

4.10 Confidence in key topics covered

After Connect

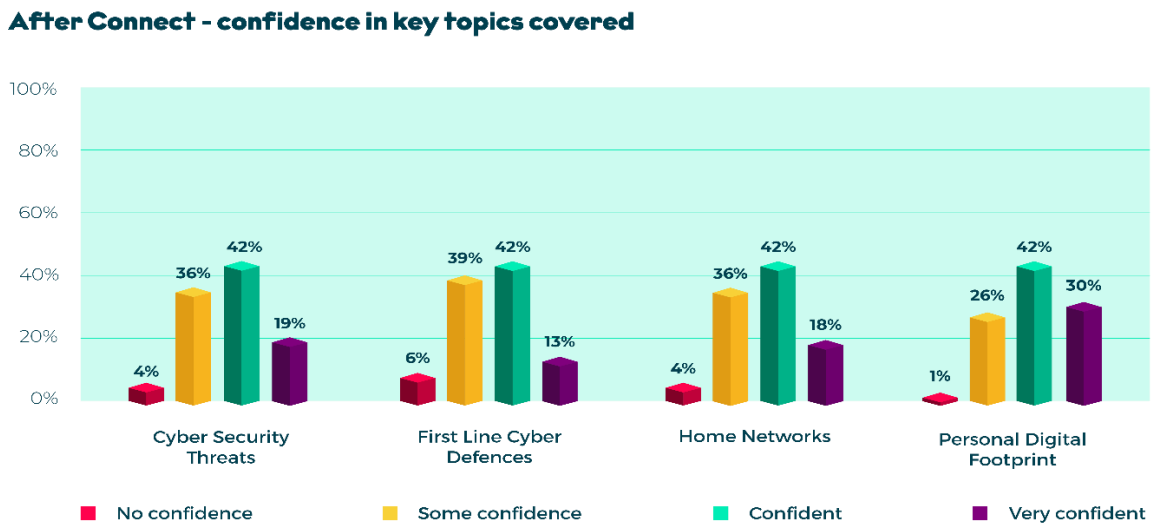
- On average, most learners scored higher levels of confidence in the area of 'personal digital footprint' – this was backed up by many additional comments on how much more knowledgeable learners felt in the area of personal online security and the impact of this on their daily lives.
- Most learners have moderate to high confidence in all topics taught despite many learners having no previous technical experience.
- The highest no confidence score related to 'first line cyber defence' – although only a difference of 2% between this and the other areas.

Learners offered a wide range of comments to support their scores, with the key themes following the Connect course including:

- Feeling more confident on a personal level rather than a business level.
- Felt they'd learned a lot but still not enough to feel confident.
- Still need to improve knowledge to help with confidence.
- Realise there is still so much more to learn.
- Need to practice more to consolidate.

- Need time to digest, read and research more.

A number of learners expressed how much they enjoyed working with like-minded people; learning alongside those with similar interests and that there was a real advantage to working in groups to do practical hands on activities to help embed the learning.



Total number of respondents: 137

Decimal places have been removed for data cleanliness – those at .5% or above are rounded up; those below .5% rounded down.

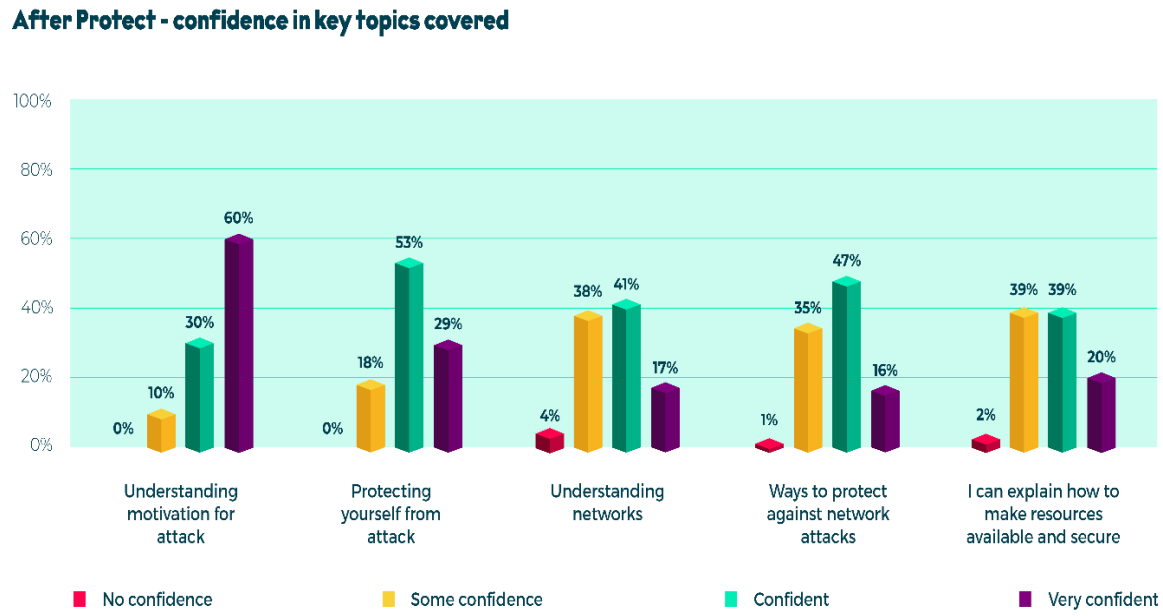
After Protect

- On average, most learners scored higher levels of **confidence** in the areas of 'Cyber Security Threats' and 'First Line Cyber Defences'.
- Most learners have **moderate to high confidence** in all topics taught despite many learners having no previous technical experience.
- **Only 4%** (4 learners) reported **'no confidence'** in any topics – linked directly to 'Home Networks', 'Personal Digital Footprint' and 'Making resources available and secure'.

A recurring theme within the additional comments shared following the Protect course is that learners found the 'networks' element of the content difficult and many commented on how much more they would need to practice this aspect to become confident. This is reflected in the scoring that we see below, with Home Networks scoring the lowest in terms of confidence of all the five topics covered.

At this stage in the programme we would expect to see learners begin to find the content more technically challenging, as the context moves from a personal security aspect to more of a business and commercial view of cyber security and its importance and impact on a much wider scale and level. This progression in content naturally means some learners find the shift harder to understand as it requires a higher level of capability and skill.

At this stage the hands-on technical labs become a key part of the programme, where learners are able to try out the skills and knowledge they've learned in the theory element of the session and put things into practice in a safe learning environment, closely monitored by the expert facilitators. Again, these labs featured highly in the learner feedback as being a positive key element of the Protect course.



Total number of respondents: 93

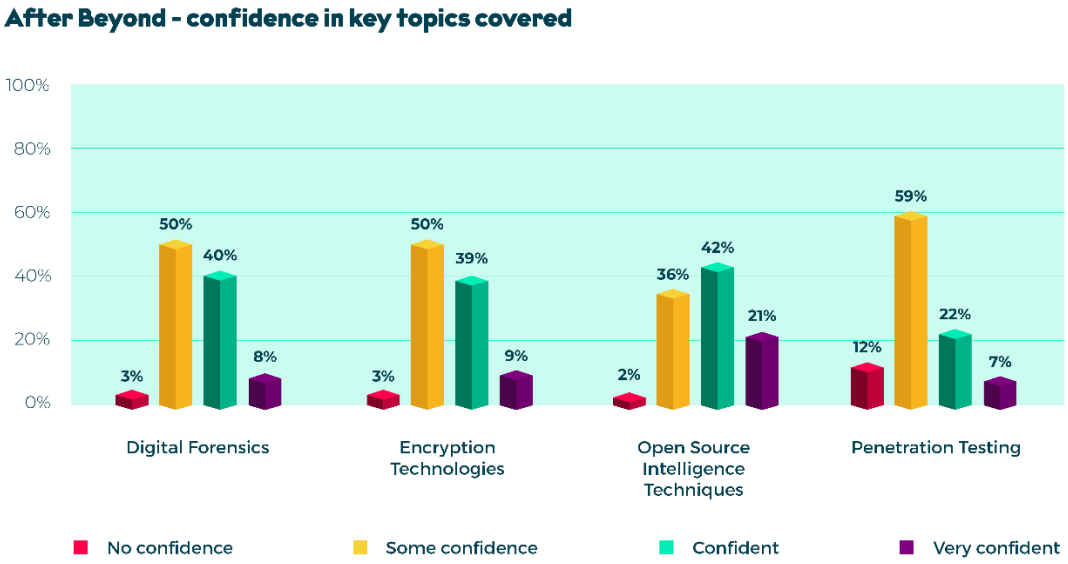
Decimal places have been removed for data cleanliness – those at .5% or above are rounded up; those below .5% rounded down.

After Beyond

- On average, most learners scored the highest levels of confidence in the area of 'Open Source Intelligence Techniques'.
- Most learners have moderate confidence in all topics taught despite many learners having no previous technical experience.
- 13 learners reported 'no confidence' in any topics, with 'penetration testing' being an area of no confidence identified by 12 out of 13 learners *(including one learner who missed some sessions due to sickness)*.

Following the final course in the programme, learners are demonstrating higher levels of confidence, knowledge, and skills.

For many there is still the desire to want to practice in order to feel more confident. There is recognition that the access to Cloud Academy for ongoing learning and further development of skills will help to fill any gaps that may exist.



Total number of respondents: 101

Decimal places have been removed for data cleanliness – those at .5% or above are rounded up; those below .5% rounded down.

4.11 Overall conclusions from evaluation data gathered

In relation to the learner's levels of interest in IT/Cyber Security, the data tells us that as learners progress through the programme, those who started out initially more technically capable continue to show high levels of interest throughout.

As the courses become more challenging, we see *some* interest levels of those less technically able drop off slightly – although there is still a desire to continue to learn and develop. Those who lack technical competence but have confidence at this stage, start to explore the wider range of roles that are less technical as they are still very much interested in the field of cyber security overall.

Those who report less interest at the end of the programme are the learners with the least amount of capability, skills and knowledge. What the data tells us here is that those with limited capability will feel out of their depth and so lacking in interest and confidence.

In terms of levels of motivation to continue to develop, this has remained at a fairly consistent and high level from recruitment right through to the end of the programme.

This aligns with learner's reasons for embarking on the programme in the first place – such as to re-skill or up-skill or to gain a job in the market.

Regardless of their level of capability, knowledge, and skills, the motivation to continue to develop does not appear to be directly affected.

Those who may ultimately decide that cyber security is not the future for them, remain energised and willing to continue to learn in order to develop.

Sign up levels to Cloud Academy are further evidence of this, with a total number of 138 out of 143 (as of 16.04.21) learners progressing onto the platform to continue to develop their skills.

When it comes to levels of confidence to apply for an entry level cyber security role, we see a big shift between the start and the end of the programme.

At the start of the programme, confidence levels are low. Immediately after Connect they show a sharp rise as people start to realise that a career in cyber security *could* be an achievable reality for them.

As the programme starts to become more demanding and challenging, confidence levels drop off a little - then rise again in the final stages as learners see their capability and knowledge improve and develop further and they are able to see the distance they have travelled in terms of their own learning.

The guest speakers on the programme help in this context to share their own experiences and knowledge of working in a cyber security environment – and that sharing of real-world examples is crucial to enable learners to make decisions for themselves about their future careers.

These levels of confidence were one of the key aims for this pilot programme, at the end of which we see that most learners have some level of confidence to apply for a role in cyber security – only 6% saying they have no confidence.

It is clear from the comments that more hands-on practice and continued learning is required by many for those confidence levels to continue to rise.

In relation to learner attitudes, the overall attitude towards cyber security is generally a positive one throughout the entire learner journey.

As confidence and capability levels increase, attitudes become more focused on whether the learners can see themselves working in cyber security as a future career – another key aim of the programme.

The data tells us that while these attitudes do not greatly shift, over the course of the 6-week programme learners gain a much clearer idea of whether a future in cyber security is something they wish to pursue. This is demonstrated in the previous comments regarding levels of confidence to apply for an entry level cyber security role.

Similarly, while most learners had a limited understanding of the expectations of a role in cyber security prior to starting training, progression through the six weeks shows this understanding develop and deepen.

The data tells us that they become more aware of the variety of roles available in this field and the guest speaker sessions further enhance this awareness and understanding, providing a more detailed view of careers available.

Finally, in terms of overall course satisfaction, our data shows that an average of 92% of learners were consistently either satisfied or very satisfied with their course. In addition, an average of 90% of learners said they would recommend the programme to their friends and family.

4.12 Programme Withdrawals

A total of 57 learners withdrew from the programme. The peak time for withdrawals was the transition between Course 1 and Course 2. Despite interest levels rapidly developing as a result of Course 1, it also gave enough time for learners to grasp the requirements and commitments involved, and some felt they would be unable to sustain this.

31 learners had to withdraw due to external commitments obstructing their ability to complete the programme. These commitments consisted of managing personal health & wellbeing (such as contracting Covid-19), care responsibilities (primarily childcare), moving house, or job commitments. Of the learners who shared withdrawal reasons, job commitments were the biggest reason why learners decided to withdraw from the programme. Particulars such as shifts opening up again, accepting job offers or work patterns changing formed the primary reasons. As a key factor in learners being attracted to the programme was the programme's ability to help spring board participants into employment, combined with the unemployment and insecurity generated from the pandemic, it is expected that some learners prioritised work commitments over the programme.

Of the remaining withdrawals, 2 learners expressed that the course was not right for them, 2 experienced too many technical difficulties at home (poor internet connection) and 22 provided no reason for withdrawing.

From the data we can conclude:

- The challenges presented by Covid-19 regarding unemployment and lack of job security means learners are unable to commit to unpaid course over paid offers of work or changes to work schedules.
- The challenges of finding childcare and family care heightened by Covid-19 and home schooling mean some learners are unable to balance these responsibilities with course commitments.
- Gathering information about withdrawals can be difficult to obtain.

4.13 Departing Skills and Knowledge

To support programme participants on their future journey, learners were provided with:

- A supporting paragraph to articulate skills and knowledge to future employers.
- A certificate outlining the key knowledge and skills gained.
- Cloud Academy training to develop and measure knowledge and skill.

Supporting Paragraph

I have successfully completed the DCMS Cyber Skills Kick Start programme and achieved the Foundation Certificate in Cyber Security. This is a nationally recognised cyber security qualification awarded by APMG.

This course has equipped me with an understanding of the digital world and insight into how technology systems and data flows are connected. This enables me to inspire others to consider the cyber security implications of their work and to become an advocate for best practice security by design.

The qualification proves that I have a solid foundation knowledge of standard security practice, approaches to encryption and penetration testing techniques and demonstrates that I have an aptitude for developing as a cyber security professional. The additional understanding of the legal and ethical implications of technology applications in the real world mean I am confident in considering possible attack vectors and responses to them.

Having worked as part of a diverse team on solving real-world issues I have shown that I know how to apply the cyber security knowledge and am now ready to develop my skills further.

The Cyber Launchpad certificate outlines the key knowledge and skills learners possess:

Cyber Connect

- Identify the source and impact of common Cyber Security threats.
- Define and apply first line cyber defences.
- Demonstrate an ability to construct, configure, and secure a home network.
- Take steps to manage and secure personal digital footprints.

Cyber Protect

- Explore the motivation for attack.
- Protect yourself from attack.
- Develop knowledge and understanding of networks.
- Describe and demonstrate ways to protect a network from attack.
- Demonstrate your understanding of how to make resources available and secure.

Cyber Beyond

- Implement Digital Forensics.
- Understand Encryption Technologies.
- Use Open Source Intelligence Techniques.
- Perform Penetration Testing.

4.14 Cloud Academy Summary

The data is true as of 15.04.21.

138/143 learners are active on Cloud Academy, showing that learners really are motivated to continue to develop. 12 learners have engaged with the consultation opportunity to ask for recommendations on courses, content, or exams specific to their interests and skills.

Total hours spent on the platform by learners: 566 hours and 23 mins.

This is an average of 5 hours 20 mins per learner. The median is 2 hours 40 mins and the most a student has spent on the platform is 32 hours! We'd expect the FCCS learning path to be 6 hours or more to complete.

Top Learning Paths:

A total of 216 learning paths have been started with 86 now completed. Out of the 138 users, 109 of them are taking one of the advised Cyber specific pathways (FCCS or Cyber Fundamentals) while others are now building on the Cloud fundamentals and choosing vendor specific routes, including 11 users on the Microsoft Azure certification prep. This pathway is the first step to becoming an accredited Microsoft architect or to a Microsoft security specific role.

Learning Path	Time Spent (hours/mins)	Users Started	Users Completed
Foundation Certificate in Cyber Security	*306h 47m*	*94*	*57*
Cyber Fundamentals Pathway	*7h 39m*	*15*	*13*
AZ-900 Exam Prep: Azure Fundamentals	8h 40m	11	0
Introduction to Ethical Hacking Tools	17h 28m	7	2
Python Fundamentals	1h 53m	6	0
Azure Fundamentals	4h 50m	4	4
Preparation for the CISSP Cert	2h 12	4	0

Time based on the total, collective time spent by learners.

Top 5 skill areas:

Security	418/1000 *
Cloud Fundamentals	396/1000
Networking	370/1000
Compute	315/1000
Business Skills	279/1000

*45% of the 138 active learners would now be considered to have intermediate skill and knowledge in this area from their scores in security (when compared to other clients on CA and the marketplace).

CA has three levels beginner, intermediate, and advanced. At intermediate level we introduce scenarios and learners are asked how to solve something, developing skill, rather than the beginner questions on facts, definition etc. Learners at an advanced level would be expected to score 667 points and above. The top 10 learners are scoring between 547 and 595 demonstrating they have the knowledge and skills to progress to advanced levels within Cloud Academy.

4.15 National Averages

Taken from:

Ipsos MORI | Cyber security skills in the UK labour market 2021. The report concludes that the cyber sector workforce is not diverse. On gender diversity, it falls behind other digital sectors.

- 17 per cent of the workforce come from ethnic minority backgrounds, falling to just 3 per cent of those in senior cyber roles (i.e. those typically requiring 6 or more years of experience)
- 16 per cent are female (vs. 28% across all digital sectors), falling to 3 per cent in senior roles

Decrypting Diversity: Diversity and Inclusion in Cyber Security. The NCSC and KPMG UK Joint report also highlights the lack of workforce diversity specifically around gender and those coming from lower socioeconomic backgrounds.

Gov.uk report on Schools, pupils and their characteristics shows the current statistic for students eligible for free school meals.

End of Supporting Data