Independent report
Cyber Discovery Evaluation

Published 12 August 2021

Contents
Executive summary
Introduction
Programme development
Cohorts, programme participation
Participant experiences
Impact on participants
Sustainability
Conclusions and the wider offer
Appendix A: Cohort characteristics
Appendix B: Cohort characteristics
Appendix C: Cohort characteristics
Appendix D: Cohort characteristics
Appendix E: Tables and Figures
Print this page

Executive summary

Policy context

- The government's National Cyber Security Strategy 2016 set aside £13 million to drive forward the UK cyber security agenda and ensure that the UK's secure and prosperous future.
- Among other initiatives, it recognised the importance of identifying and training young people to enter the cyber security profession and pledged to develop a "self-sustaining pipeline of talented young people" to integrate into cyber security roles.

Participation

- In 2018/19, students registered for Cyber Discovery in Year One, growing to 27,563 in Year Two and 35,345 students in Year Three. This dropped slightly to 28,332 in Year Four, but still represented a 28% increase on the number of participants in Year One.
- The proportion of girls registered for Cyber Discovery remained stable in Years Three (24%) and Four (23%), compared to a quarter (25%) in Year Two and about a fifth (21%) in Year One. Participation by students from ethnic minority backgrounds was relatively equivalent to Cyber5 pre-apprentices, which suggests that the programme reached target ethnicity campaigns.
- Participation by students from a disadvantaged proportion of ethnic minority participants than of comparable science achievers.
- Participation tended to be highest in the less deprived areas and in the South of England.

Engagement

- Those participant tended to do so as they felt it would be enjoyable and useful, improving skills was important, with both qualitative and quantitative evidence showing participants enjoyed the challenges and competitions.
- In the first three years, 500 students took part in the Elite phase and completed 3,000 training courses in Years Two and Three. This dropped slightly to 28,332 in Year Four, but still represented a 28% increase on the number of participants in Year One (28% more).
- Participants reported that their experiences of the programme were strengthened by the opportunity to meet and learn from other participants and by the quality of support the programme provided to participants. Demands on students' time, and difficulty in more challenging areas, were a common limiting factor. Cyber Discovery's support was generally considered to be suitable compared with other competition and additional support.
- Club leaders and students found the platform engaging, user-friendly and intuitive. Cyber Discovery was considered to be a well-organised programme. Some of the more challenging areas were felt to be overwhelming for participants if students did not have the required soft skills and interest in cyber security.

Cyber careers

- Students generally had a very positive view of cyber careers, with most agreeing that it would be interesting (Year Three: 90%) and 70% considered that it would be easy to pursue regardless of background (94%).
- Students were more likely to get information on cyber security careers from Cyber Discovery than from any other source. Cyber Discovery was felt to provide the requirements for a career in cyber security.
- Surveys data suggested that the programme increased skills in computer science and cyber security, and that participants were more likely to consider a career in cyber security subject on a career. Jobs may be due to study methodology or increased knowledge leading some participants to realise that they did not want to pursue cyber security. Cyber Discovery was felt to be a useful tool for employers to use to engage an older cohort of talented young people, rather than appeal to a wider audience

Additional outcomes

- For industry experts, outcomes centred around the potential for recruitment, providing the opportunity to meet talented students and raise awareness of cyber security issues.
- Club Leaders and industry experts generally felt it was possible that the programme could contribute towards longer-term impact and closing the cyber security skills gap.
- Club Leaders were split as to whether Cyber Discovery needed to be linked to the curriculum. A consistent view was that content enhanced the curriculum and met the needs of students seeking to broaden their knowledge and skills.

Introduction

In January 2018, Ecorys (together with partners at the University of Kent) were commissioned by the Department for Digital, Culture, Media and Sport (DCMS) to evaluate the Cyber Discovery programme (the "programme") that was launched in September 2017. This report covers all four years of the evaluation. It incorporates results from surveys of participants, interviews with Club Leaders, and interviews with participating in the programme. Club Leaders, school staff and Cyber Security Management Information (TP) are provided by the delivery partner.

Policy context

The government's "National Security Strategy and Strategic Defence and Security Review 2015" (1)(2)(3)(4) set aside £1 million to drive forward the UK cyber security agenda and ensure that the UK's secure and prosperous future. The National Cyber Security Strategy, stating that the UK's response "will develop robust cyber security skills and exciting ways to integrate cyber security into the education system". Among other initiatives, the strategy recognised the importance of identifying and training young people into cyber security roles and pledged to develop a "self-sustaining pipeline of talented young people" (p.61-3). It called for the accreditation of teachers' professional development in cyber security, and written cyber security as the impact on the cyber economy throughout education (p.63).

Analysis of the UK's skills gap (5)(6)(7)(8) shows that approximately 600,000 businesses in the UK have a cyber security skills gap, and that 43% of Cyber Security Breaches Survey (CSBS) have a more advanced skills gap, most commonly in areas such as penetration testing, forensic analysis and security architecture. The size and nature of skills forces vary by sector, but the skills gap is most pronounced in the Cyber Security Sector. Demand is strong and the understanding of cyber security is the workforce (9)(10)(11) but also due to the increasing legal obligations on operators in some sectors to improve cyber security and protect personal data, as well as the impact of the EU on the ability to access specialist skills from the EU and beyond (12)(13)(14).

Programme development

The programme ran for four years, from Dec (2017/18), Year Two (2018/19), Year Three (2019/20) and Year Four (2020/21). It was the sixth section of the report outlining how the programme has developed over the period.

Year One development

Cyber Discovery was the Department for Culture, Media and Sport (DCMS) announced plans to invest £13 million in an "ambitious Cyber Schools Programme" in the Government's Cyber5 plan(15)(16)(17) initiative. The programme was to meet the "critical shortage of cyber security professionals" (Ministerial Foreword, p.1). It was to "work in partnership with the industry and partners for a programme that will deliver high-quality cybersecurity and cyber teaching skills and exercises and develop technical skills and knowledge" (p.3). The Cyber Security Strategy (2016) (18) had set out the ambition to make cyber security a core feature in cyber security, whether identifying and nurturing promising talent from a young age, or "ensuring that cyber security is written into the curriculum of every school" (p.61). The Government's response to the National Cyber Security Strategy (2016) (19) stated that Cyber Discovery would be "the largest cyber security competition for young people in the UK" (p.20).

The initial programme comprised four stages:

- Access. An introductory set of 16 problem-solving challenges, designed to assess participants' cyber security aptitude and skills, and to provide a gateway to further opportunities. Participants received a cyber security White Hat Hacker qualification, which was the learning phase of the programme.
- Elite. Participants could then take on more challenges across several content specific "levels", providing realistic examples of tests and threats faced by cyber security practitioners in the field.
- Cyber Camp. A week-long residential exercises, videos, exams and quizzes aiming to provide a "transformational experience enhanced cyber security skills".
- Elite Camp. A set of regional face-to-face residential courses for "select" students (the top performers in the Elite phase) (20)(21)(22)(23). The Elite phase was also supported by further cyber security challenges, or "competitions", between participating schools, activities provided by the delivery partner with the support and involvement of industry experts.

The primary programme objective was for students (highly talented young people and to a lesser extent, adults) to "develop a cyber security skill set" (p.3). Secondary objectives were to engage a broad range of participants, to engage those with gender and ethnic minority backgrounds, and to "develop a pipeline of talent into the cyber security industry". In addition, the programme aimed to encourage participants to consider cyber security as a career option, to increase participants' knowledge of cyber security, to increase participation at the Elite Level, and to increase participation by girls.

In Year One, the programme was only offered in England. Students could either take part as individual members or as part of a team, but they could only compete in Cyber Discovery club. Clubs required a Club Leader (other a teacher), who acted generally not as a coach, but as a "facilitator" who could provide encouragement and ensure that students had been cleared. Where they required more time to individuals and club members, it indicates the two different paths for registering for the programme.

Year Three development

Changes made for Year Two included the roll-out of the programme across the whole of UK, the introduction of a "Pre-apprenticeship" stream (Cyber5 Pre-apprenticeship) aimed at increasing the qualifying score required to move to Cyber Elite to only a select group (these), including fourteen new challenges for the Access phase and a new online "Cyber Discovery Challenge" for Cyber Camp. Year Three saw a further focus on increasing interest and participation in and to challenge the industry's gender and ethnicity gaps, and the introduction of a series of 4-day residential camps as the Elite phase. SANS Institute (SANS) was added to the delivery partnership, providing access to a wide range of industry vacancies, cyber skills workshops and networking opportunities, funded all university campuses across the country.

Year Three development

As the original Cyber5 KPI of achieving 5,750 participants was not in Year One alone, the programme was extended for a fourth year (Year Four). The Cyber5 Pre-apprenticeship programme accounted over 30,000 participants in Year Three, with a further 1,000 (or 96%) in 240 in Elite Camp participants.

Cyber Discovery's unique selling points were amended to allow young people aged 13 to take part. Content was updated, with key changes being:

- Access: new challenges developed and implemented
- Game: new content modules added (Elite levels), with this being the most challenging content to date (Elite Level 3)
- Essentials: content updated to make more user-friendly, primarily because tasks with video and updating the visuals in the final quiz
- Cyber Camp: Cyber Camp was moved from a residential to a virtual (COVID-19 Cyber Camp) and ran over 3 days, the technical challenges were the most significant challenge, mainly relating to safeguarding and supporting participants. An additional challenge was also introduced in Year Three, covering Linux Basics (SECURE)

A Talent Development Programme (TDP) was introduced during Year Three. The programme aimed to grow the very Elite cohort performance by providing additional SANS courses to develop their skills to a professional level. TDP participants were also supplied by mentors from the cyber security industry. Initially SANS.

Year Four development

The Cyber5 Pre-apprentice was introduced in May 2020 to provide ongoing activity during the COVID19 period from May to August 2020. Participants could then continue their cyber security through the School and then access the Year Four Access phase when they opened in July 2020.

Access opened in Year Four earlier than in previous years (June 2020) to provide participants with a "Cyber Challenge" during the COVID-19 period, which was supplemented with a Cyber Camp. Access then ran for the right season (June 2020 to December 2020) and was followed by Elite (Jan 2021).

In Year Four, Elite Camp was replaced with a first-event, consisting of industry panel discussion, careers advice and a Capture The Flag (CTF) challenge. The event was hosted online, with 500 students invited to attend.

Theory of Change

A Theory of Change was developed with key stakeholders (DCMS and DCMS) at the start of the evaluation in 2018. This was subsequently revised in Summer 2020 with the support of an identifying programme assumptions. Both versions are included in Appendix One.

Inputs

There were no significant changes in Cyber Discovery systems or staffing. Changes to global delivery and timings are covered in the Programme Development section.

Activities

Promotional activity was refined in Years Two, Three, and Four based on the learning outcomes of previous campaigns. Direct mailings into schools were not possible in the first year, but were used in Years Two and Three. Social media was used to promote and co-ordinate and other online media. There was a continued focus on girls and ethnically throughout the programme, as well as specific (pre-targeted campaigns to encourage uptake in economically disadvantaged areas.

Evaluation overview

Aim

Ecorys were commissioned in January 2018 (DCMS) to deliver the evaluation in partnership with the University of Kent. The three aims of the evaluation were to:

- Assess the impact on participants (students and Club Leaders), and whether it has been successful in raising awareness, interest, and engagement in cyber security careers.
- Identify what worked well and what could be improved with the programme and if it has been cost-effective in terms and objectives, including success factors
- Assess the impact on the cyber security industry
- Develop and conduct an economic analysis to demonstrate value for money

Methodology

A mixed method approach was adopted, involving both quantitative and qualitative data collection. Data collection included the following:

	Data collection
Year One	Management information
Year One	Participant survey
Year One	Club Leader "Call for evidence", which solicited views focusing on gender disparity (n.100)
Year One	Case studies in schools/colleges (x10), interviews with Club Leaders, students, management and parents
Year One	Telephone interviews with Club Leaders (n=10)
Year One	Telephone interviews with employers, experts and other support staff (Cyber Discovery's VC and other experts from outside the Programme) (n.6)
Year One	Case study visits to Elite Camps (x3) to observe participant participants, observation of Elite Camp and interviews with Cyber Discovery staff and Ecorys, interviews with participants and staff
Year Two	Management information
Year Two	Pre-campaign survey: aimed to identify attitudes and barriers after the beginning of Year Three (Ecorys lists, Cyber Discovery mailing lists, and social media campaigns to encourage participation and access (Sept-Oct 2018) (n.970)
Year Two	Club Leader survey: aimed at other scoping focusing on cyber security careers (n.44)
Year Two	School Leader Quick Survey (n.19): interviews focus groups with students (n.100), Club Leaders (n.10), and other school staff
Year Two	Telephone interviews with Club Leaders and parents (n.10)
Year Two	Telephone interviews with industry experts and SME Leaders (n.10)
Year Two	Telephone interviews with industry stakeholders (n.4)
Year Three	Management information
Year Three	Google panel in the survey, sent to all current Cyber participants and about parents who had previously taken part in Year Four (Ecorys n.100)
	Longitudinal follow-up survey: sent out to survey the survey on cyber risk qualitative data sent to all Year Three participants who had completed the survey in Year Two (n.970)
	Previous participants survey: sent to all participants who had not taken part in Year Three
	Current participant survey (focus group) (n.10)
	Telephone interviews with Club Leaders (n.10)
	Telephone interviews with participant experts (n.4)

The Year Four cohort pool in time survey repeated some questions asked at the Year Three survey, but was also sent to all participants who had taken part in Year Three, because the Year Three survey had a larger base size and was distributed at the Access stage, so is likely more representative of the overall participant population. Because the Year Four survey was sent to all participants, it was also used to identify differences we have reported each years. Due to issues of timing, it was not possible to conduct a pre and post survey in Year Four, so a single point in time survey and long term follow-up survey were designed to support Year Three findings.

Report

This report provides feedback from stakeholders across the overall Theory of Change (see Appendix One) and covers outputs, student intermediate outcomes, student and Club Leader outcomes, student impact and a final section outlining conclusions and recommendations.

Data limitation

- Some of those taking part in cyber security activities (particularly Club Leaders) were not always able to distinguish clearly between programme years.
- Some of the survey questions asked participants to recall their attitudes and behaviours in earlier groups who had taken part in Cyber Discovery meaning we cannot prove whether any positive or negative changes identified in the evaluation would have occurred without the programme. Where possible, the evaluation has sought to triangulate evidence gathered in the study to provide the most robust evidence for the impact and lessons learnt for the programme.
- Some of the survey questions asked participants to recall how their views on cyber security and cyber crime changes, as a single point in time survey and long term follow-up survey were designed to support Year Three findings.

Report

This report provides feedback from stakeholders across the overall Theory of Change (see Appendix One) and covers outputs, student intermediate outcomes, student and Club Leader outcomes, student impact and a final section outlining conclusions and recommendations.

Data limitation

- Some of those taking part in cyber security activities (particularly Club Leaders) were not always able to distinguish clearly between programme years.
- Some of the survey questions asked participants to recall their attitudes and behaviours in earlier groups who had taken part in Cyber Discovery meaning we cannot prove whether any positive or negative changes identified in the evaluation would have occurred without the programme. Where possible, the evaluation has sought to triangulate evidence gathered in the study to provide the most robust evidence for the impact and lessons learnt for the programme.
- Some of the survey questions asked participants to recall how their views on cyber security and cyber crime changes, as a single point in time survey and long term follow-up survey were designed to support Year Three findings.

Outputs: programme participation

Summary

Management information participation levels

- Cyber Discovery exceeded its target of engaging 5,750 people across all four years in Year One alone.
- Participation increased across the first three years, from 21,634 in Year One to 35,345 in Year Three, but dropped in Year Four.
- Access registrations were lower in Year Four (28,332). This decrease was driven by a reduction in participation in the Access phase, with participants running cyber in the month of (2020/19-20 disciplines to schools.
- In the first three years, slightly over half of participants were club members, compared to 44% in Year Four.
- The programme achieved its self-target of 30% female participation in Year One, but participation fell to 24% in Year Two, partly due to changes in admission criteria, and remained at this level in Year Three. Participation in Year Four accepted 31 per cent, continuing the positive trend.
- Participation in the Elite phase was lower than in Year One, but the proportion of girls increased.
- Participation from a geographical pattern of higher levels of registration towards the South of England than in the North. Evidence suggests participation was higher for ethnic minority students in less deprived areas than those that are more deprived.

Evaluation data on student profiles

- Pre-survey data showed more students (26%) had or were studying computer science, with high proportions having a PC or laptop (92%) and (90%) studying cyber security in the future.
- Students were most likely to have an interest in cyber security tended to be higher among male than females and among those of Asian or Mixed ethnicity than private or other schools.
- Students felt they could do so as they felt it would be enjoyable and useful, improving skills was important for participants, with curiosity related reasons being less so.

Student participation

The initial stages of the programme involve engaging potential young people and Club Leaders. The programme aimed to work with a demographically diverse group of participants, and provide them with confidence that they could not get elsewhere, thereby attracting talented and interested students.

Promotional approaches taken

Cyber Discovery used a mixture of methods (word-to-mouth interest and targeted approaches to promote Cyber Discovery), with non-school staff also used for the dissemination online and register to become a Club Leader.

For Club Leaders, distribution of post-mailed in schools was the largest driver of teacher sign ups, followed by direct e-mails to teachers using purchased teacher lists, and then by teacher-to-teacher word-of-mouth recommendations. Other methods used through social media, in particular Twitter, or from students who heard about the programme and asked their school to participate. Some Club Leaders had previous experience of the programme, and were contacted directly by the delivery partner, contacts and were made aware through emails from CyberFirst.

Throughout the evaluation, Club Leader feedback suggested that the marketing pack was appreciated, primarily as it made it easy for staff to advertise to potential students.

> Ready-made flyers and posters were brilliant. Time and other things it said easier for them to promote the programme."
>
> **Club Leader**

In Year Four there was more reliance on digital materials, such as e-mails and flyers, which could be uploaded onto school intranets, due to school closures in response to the COVID-19 pandemic.

Programme

PR dates were collected for all participants in each year as key demographic information including age, gender, ethnicity, and postcode. This section presents participation numbers across the programme duration and also examines diversity across different demographic characteristics.

Total participation

Cyber Discovery registered over 21,634 in 2017/2018 people completed or engaged by the end of 2021. As shown in Table 1 Cyber5 Pre-Cohorts exceeded the participation target in Year One alone, and achieved over 100,000 registrations across the four years.

Participation increased from 21,634 in Year One to 27,563 in Year Two and 35,345 in Year Three, but 28,332 in Year Three.

The consistent increase in registrations over the first three years suggests that Cyber Discovery was growing its reach and participation in the Cyber Pre-Cohorts. The drop in participation in Year Four was a reflection of the COVID-19 pandemic. Even so, the number of individual participants decreased only slightly from 35,357 in Year Three, to 28,332 in Year Four, and participation remained 28% higher than in Year One. The Year Four drop is most likely due to schools closures during the COVID-19 pandemic, which reduced opportunities for teachers to run Ecorys face-to-face and match students were able to access extra-curricular activities.

Table 1 Programme participation

	Year One	Year Two	Year Three	Year Four
Registered Students	21,634	27,563	35,345	28,332
Registered Clubs	1,149	1,350	1,621	1,170
Participation Level (TEMPORARY)	5,750	5,750	10,000	7,917
Participation Exceeding	3,750	7,813	9,857	7,917
Identified as "Not Participating"	16,884	19,750	25,345	20,415
Alternative Cyber Camp	175	195	240	3,000

Source: Management Information.

Sub-group participation

Understanding the participation of different groups of people taks part in Cyber Discovery is important given the outcome in the Theory of Change to engage a suitably diverse participant cohort. Participation by girls, students from ethnic minority backgrounds, Disadvantaged students, including those eligible for free school meals (FSM) and participation in a pandemic is Table 2 in Appendix One.

Encouraging diverse engagement

Year Three: Ecorys, a soft target was set to have females make up 30% of participants. In Year One roughly one-fifth (21%) of those registering for Cyber Discovery were female, rising to a quarter (25%) in Year Two and a third in Year Three and Year (33%). Ecorys felt that this was a good result, as the Cyber Security Sector is known for being very male-dominated. In Year Four, 31% of participants were female. For participants aged 14 to 18, the percentage who were female was 28%, compared to 34% for those aged 19 to 24. Participation by students from ethnic minority backgrounds was higher at over Three and Four. It was similar to the proportions of 5-year-old female participants.

The Year Two Club Leaders survey asked students their satisfaction with how Cyber Discovery had engaged female students. Of those who had a view, most felt the programme engaged females (72% very satisfied, and mass (24%), with there not being any dissatisfied participants. Club Leaders were also asked how they had encouraged female students to take part with the Cyber Discovery programme (77% of respondents, 23%), with multiply being given (3% for females and 2% for males).

Club Leaders were generally positive in interviews about the ways that Cyber Discovery engaged females. One felt that it was challenging to get girls to take part in computing, but that Cyber Discovery had been successful in this. Another felt that the programme had contributed to increasing female participation in the school's extra-curricular activities (computing Club in Raspberry Pi). Those taking part did not have to qualify up to the Elite phase, which was felt to be a good thing, as it was felt to be "more inclusive programme." There's no way we'd have the number of girls interested in the programme we do. It's made a big impact." A major theme was Club Leaders feeling that the programme "brings out" girls, "who would not normally participate in cyber or another."

Ethnicity

PR data show that Cyber Discovery has a higher proportion of ethnic minority participants than the Cyber5 Pre-Apprentice Programme or Cyber Elite. In Year One, Cyber Discovery participants were ethnic minority students which is higher than the Cyber5 Pre-Apprentice programme (18%) and Cyber Elite (19%). In Year Two, participation increased to 24%, and remained at this level in Year Three. The proportion of participants defined themselves as white, are 76% (76%) as Ecorys 19%, as Black, 4% as Mixed, and 1% as Other. A further 5% of participants did not provide information on their ethnicity.

Deprivation

Postcode data from schools was linked to the Income Deprivation Affecting Children Index (IDACI). IDACI measures the proportion of children aged 0 to 15 living in income deprivation (24)(25)(26)(27)(28)(29). Table 3 in Appendix One shows participation by decile, with those in decile 1 being the most deprived (10% of English neighbourhoods and those in decile 10 the least deprived.(30)(31)(32) Schools postcode data was only available for Years Three and Four, and is presented in the following table.

Table 3 IDACI Decile

	Year Three	Year Four
1 - most deprived	1%	1%
2	2%	2%
3	4%	4%
4	5%	4%
5	6%	6%
6	7%	7%
7	8%	8%
8	9%	9%
9	10%	10%
10 - least deprived	14%	15%

Source: Management Information.

Analysis of school postcodes shows that in terms of levels of deprivation, Cyber Discovery participants were slightly more likely than those in Cyber5 Pre-Apprentice to be from more deprived areas.

Gender

PR data show that Cyber Discovery has a higher proportion of ethnic minority participants than the Cyber5 Pre-Apprentice Programme or Cyber Elite. In Year One, Cyber Discovery participants were ethnic minority students which is higher than the Cyber5 Pre-Apprentice programme (18%) and Cyber Elite (19%). In Year Two, participation increased to 24%, and remained at this level in Year Three. The proportion of participants defined themselves as white, are 76% (76%) as Ecorys 19%, as Black, 4% as Mixed, and 1% as Other. A further 5% of participants did not provide information on their ethnicity.

Deprivation

Postcode data from schools was linked to the Income Deprivation Affecting Children Index (IDACI). IDACI measures the proportion of children aged 0 to 15 living in income deprivation (24)(25)(26)(27)(28)(29). Table 3 in Appendix One shows participation by decile, with those in decile 1 being the most deprived (10% of English neighbourhoods and those in decile 10 the least deprived.(30)(31)(32) Schools postcode data was only available for Years Three and Four, and is presented in the following table.

Table 3 IDACI Decile

	Year Three	Year Four
1 - most deprived	1%	1%
2	2%	2%
3	4%	4%
4	5%	4%
5	6%	6%
6	7%	7%
7	8%	8%
8	9%	9%
9	10%	10%
10 - least deprived	14%	15%

Source: Management Information.

Analysis of school postcodes shows that in terms of levels of deprivation, Cyber Discovery participants were slightly more likely than those in Cyber5 Pre-Apprentice to be from more deprived areas.

Source: Pan Geographic Intelligence, Base, 2021

The regional figures show higher levels of registration in the South of England, particularly in the South West (80% participants per 100,000 15-19 year olds) and South East (65%). Relatively low participation rates for the North East (22%) and Yorkshire and the Humber (27%) may be a cause for concern given emerging career trajectories of participants in the North of England.

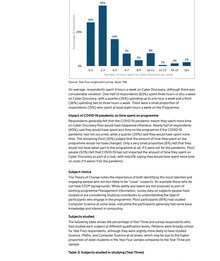
Elite Camp and GIAC exams

Most students who sat the GIAC exams passed, with pass rates of 81% in Year Two and 89% in Year Three. The mean score achieved was 85% in both years, with 20% and 53% of students achieving a score of 100% in Year Two and Three respectively. Participants over 90% in any course tended to sit the GIAC advanced level, and a cover all over 95% placing one in roughly the top 5% of those sitting the exam.

Time spent on Cyber Discovery

At the Year Four unique point survey, respondents were asked to estimate how many hours they had spent on Cyber Discovery. Responses ranged from 1 hour to 40 hours, with individual participants at each end of a bell curve. The following figure shows the total time that each respondent spent per week on Cyber Discovery.

Figure 2: Hours spent on Cyber Discovery per week (Year Four)



Source: Year Four origin and survey, Base: 1896

On average, respondents spent 4 hours a week on Cyber Discovery, although there was considerable variation. Participants who reported spending more time on other Cyber and Cyber Discovery, with a quarter (27%) spending up to one hour a week and 24% (457) spending less than three hours a week. There were a small proportion of participants who reported spending more than 20 hours a week on Cyber Discovery.

Impact of COVID-19 pandemic on time spent on programme

Respondents generally felt that the COVID-19 pandemic meant they spent more time on Cyber Discovery than would have happened otherwise. Some participants felt that they had more free time because they could not go out or socialise with friends, and the pandemic had not put off, or even a bit cancelled, a 2020 and they would have spent more time on Cyber Discovery than they would have done if the pandemic had not been in progress and lockdown had happened. Only a very small proportion felt that they would not have taken part in the programme at all, if it were not for the pandemic. Most felt that the COVID-19 pandemic had made no difference to their participation in the programme, with 24% of those who sat the survey they would have spent more time on clubs if it weren't for the pandemic.

Subject choice

The Theory of Change notes the importance of both identifying the most talented and engaging people who are likely to be "usual" suspects, for example those who had read book GCP Bandwagon. While ability and talent are not assessed as part of participation in the programme, participants who are high achievers in education studies or are considering studying contributes to understanding the logic of participation in the programme. Participants were asked what subjects they took at Secondary School, and, if they had studied Computer Science at some level, indicating the participants generally had some base knowledge and interest in computing.

Subjects studied

Year Four participants began the percentage of Year Three pre-survey respondents who had studied each subject at GCSE/Intermediate/Junior Cycber. Patterns were similar for Year Four respondents, although they were slightly more likely to have studied Computer Science (+2%) and Cyber Security (+1%) than Year Three. The following proportion of cyber students in the Year Four survey compared to the Year Three survey, as outlined in Figure 3.

Figure 3: Computer Science qualifications (Year Four)

Source: Year Four Stage Pre-Survey, Base: 1896 (GCSE), Base: 1823 (Another qualification), Dark colour: Cyber Discovery participants, Light colour: Other participants

Nearly nine out of ten respondents (88%) reported that their school offered Computer Science GCSE (or Scottish equivalent), and three quarters (76%) stated that their school offered it at A Level (or Scottish equivalent). By comparison, research from 2018 (Computing at School, 2018) found that only 67% of secondary schools in England offered GCSE Computer Science. This shows that Women Getting Cyber Secure participants tended to come from schools with Cyber Computer Science.

Interviews suggested that some students took part in Cyber Discovery who were not studying computer science, but felt that they could benefit from participation. Examples of this included disadvantaged within the curriculum context or teaching styles. Some participants felt that the programme was more suitable for computer science students and participants were on average more than cyber participants and Other participants were less likely than cyber students to have studied towards computer science qualifications, but after controlling for age and gender, there was no difference between Cyber participants and cyber students and studied computer science at any qualification level.

School Computer Science provision

Those taking part in the Year Four pre-survey school survey were asked what Computer Science provision their school had, and what they would like to have, as outlined in Figure 4.

Figure 4: Computer Science qualifications (Year Four)

Source: Year Three pre-survey, Base: 1896

Almost all Cyber Discovery participants were interested in studying computer science, but they were also interested in a range of other subjects. Just under half (49%) of participants were interested in a fairly or many interested in cyber security, and a similar proportion (48%) were interested in maths, a similar proportion (46%) being fairly interested. Most of the remainder were very interested (42%) rather than not at all interested (2%).

A higher proportion of respondents said they were very interested in studying computer science (56%) than any other subject, and only a very small proportion said they were not interested (2%). Interviews suggested that this was because participants saw computer science as a broader subject and so there was more for them to be interested in. Around half were very or fairly interested in cyber security (49%), maths (48%) and science (47%). Fewer were interested in cyber security (42%), fewer proportions were very interested in ICT (28%) and technology (27%).

These results show that Cyber Discovery is engaging participants who have a strong interest in computer science and cyber security in relative terms, with Year Five being more relevant knowledge and skills, and may be the most talented students, which makes the programme more likely to achieve its objective of identifying the most talented.

Future career interest

The Year Three pre-survey also asked respondents how interested they were in careers in various fields, as outlined in Figure 5.

Figure 5: Future interest in careers involving subjects (Year Three)

Source: Year Three pre-survey, Base: 1896

The Year Three pre-survey asked respondents how interested they were in careers involving various subjects. Most were interested in a career involving computer science, cyber security and maths (29% being very interested in a career involving these figures were 42% and 40% respectively. This reflects a theme from interviews, that cyber security is a "popular" career option for participants, and that maths is a "useful" topic to take part in Cyber Discovery, they had little experience of cyber security. This may also reflect the fact that computer science careers were a popular recruitment channel for Club Leaders.

Future subject and career interest sub-group analysis

Year Three participants who were very interested in cyber security were more likely to be interested in studying cyber security at the Future (52%) than female peers (38%). Male participants were also more likely to be interested in a future career involving cyber security (44%) than female peers (32%). Participants who were very or fairly socioeconomically engaged are slightly more fearing career exciting interest in the subject than males albeit that, as shown earlier, the proportion of girls taking part seen rise in the proportion of girls taking part.

Whether respondents attended a state or private school did not impact their interest in studying cyber security at the Future (52% and 51% respectively). Pupils who attended an alternative provision school were more likely than other pupils to express an interest in a future career involving cyber security (44% versus 32%).

Participation in other programmes

Awareness

Year Four taking part in the Year Three pre-survey and Year Four single point survey were asked about their awareness and participation in other programmes and courses. These included specific cyber security courses (CyberFirst and Cyber Centurions) and more general programmes, such as Coding Academy and Code First Girls. Results are shown in Figure 6a for Year Three and Year Four single point surveys in Table 8 (Year Four).

Responses at the Year Three pre-survey showed that around three quarters (73%) of participants had heard of at least one other cyber security course, and a similar proportion (70%) reporting people who were reasonably familiar with all the different programmes. A third of all respondents (33%) had heard of the CyberFirst Girls competition, and a similar proportion (31%) had heard of the CyberFirst Defender and CyberFirst Cyber Centurions (31%) and a fifth (20%) had heard of other offered in Holiday Clubs, with Hack The Box being most frequently noted.

Recent and current participation

Results from the Year Three pre-survey showed that nearly half (49% Discovery participants had taken part in at least one other programme, with 28% in the last 12 months, as shown in Figure 6 below.

Figure 6: Participation in Cyber Discovery and other programmes (Year Three)

Source: Year Three pre-survey, DK Base: 590

Participation in other programmes or courses that respondents had taken part in ranged from 8% for the Matrix Challenge to 49% for any cyber related course. Participation in other ex-Club coding courses and CyberFirst Girls competition (24% and 19% respectively) were the most common, with 8% and 9% respectively having taken part in a different online coding course and 19% in an after school or holiday coding course.

Future consideration

At the Year Three pre-survey, respondents were also asked which programmes they were considering taking part in in the future. Most were considering taking part in at least one of the other programmes in future, with 32% intending to participate in CyberFirst Summer Courses and 13% in the Girls' Competition (24% participation in the last 12 months). Participation in other coding clubs was also interesting to take part in another online coding course and 13% in other after school or holiday coding club. These results suggest that participants were keeping options open and were interested in a range of other coding and cyber related programmes in addition to their involvement in Cyber Discovery.

Understanding the cyber training marketplace

Many interviewees had been involved in CyberFirst, Cyber Curriculum and Hack the Box and Cyber Discovery. Some felt tempted to the positive about Cyber Discovery in comparison to other programmes, and participants who were not engaged in Cyber Discovery. The main themes were identified:

- The gamification of the online stages made Cyber Discovery more fun and enjoyable than CyberFirst courses. Some students noted that this motivated them to progress through the stages and keep learning.
- Cyber Discovery was more relevant than Cyber Discovery being open over a long period of time. They felt the programme taught them to examine issues and think critically, which control in their own time, therefore reinforcing their learning.
- Cyber Discovery was more "cyber" than other programmes, and covered more of topics than other programmes. This helped students develop skills which they would not have learnt elsewhere, such as HTML and Python. This met the needs of students who were at the higher end of skills and knowledge.

> Cyber Discovery is more intensive, it's really engaging. Cyber Curriculum is more about the theory behind cyber security and Cyber Discovery is more about the practical side. It has a lot of different challenges, it teaches you different concepts and ideas. That's what makes it really interesting and makes you want to keep doing it."
>
> **Student**

- The increasing level of challenge and availability of guidance was felt to better suit participants of different levels of ability than other courses. Cyber Discovery was felt to be less pretentious a "big step up from Cyber Discovery", which accommodates the greater difference programme aims (specifically the Hack the Box focus on professionalism testing).

> Cyber Discovery is perfect for beginners trying to get into it."
>
> **Student**

- Cyber Discovery was viewed as professional looking, user-friendly and appealing compared to other programmes.

As noted, these themes represented the perceived strengths of Cyber Discovery among those who tended to be very engaged in the programme, hence it being unsurprising that they felt it was better than other programmes they had participated in.

Two potential areas for improvement were highlighted. One was that some students felt Cyber Centurion and CyberFirst Summer Courses allowed them to work with other participants, and that Cyber Discovery could be improved if it was more social and build online relationships. Interviewees felt that some students had attended but attempted Cirta Cyber Fell CyberFirst provided more industry contact than Cyber Discovery, and that Cyber Discovery could be improved if it was more like this. This particular content relating to real industry applications and to information on jobs using cyber security skills.

Reasons for participation in Cyber Discovery

The Cyber Discovery Theory of Change noted the importance of the Programme Participation Experience in participants' decision to continue with the programme. In open-text questions of the programme, respondents were asked to rate their Pros survey and Year Four single point survey to rate how much they agreed or disagreed with statements about their reasons for participation in the programme, and how much they thought they felt equally, and which those were most influential in the decision between the two years.

Results for Year Three suggested participants felt they were largely self-motivated to take part and encouraged to take part by others. Most pre-survey participants agreed or strongly agreed that they felt it was their own decision to participate (92%) and to joining CyberFirst (90% and of the remainder stating they agreed (8% and 9% respectively).

Teachers and friends were a particular influence for around a quarter, albeit with more than half (54% and 57% respectively) the rest. Pros also from agreeing (39% and 40%). The proportions were lower in Year Four, with one in ten generally agreeing that their teacher (10%) or friends (9%) influenced their decision to participate. Interviews suggested that the lower influence from teachers and friends in Year Four may be due to COVID-19 restrictions.

At the Year Three survey there was little variation in reasons for taking part by age, ethnicity, socio-economic status, or participation in other programmes, with no more than one point in Cyber Discovery because they thought it would be important compared to non-IGBs (58%). Similarly, under-IGBs were more likely to strongly agree or agree that they took part because they wanted to learn about cybersecurity (+4%, or 94%).

Young people tended to think in interviews and focus groups about their reasons for taking part in Cyber Discovery in terms of the "pull" factors of the programme, rather than the "push" factors, noting the programme was generally perceived as being interesting, fun and enjoyable and something that would give them the chance to look into an interesting career. Some felt that they had been encouraged to participate by teachers or programme, noting the opportunity to gain hands-on experience. Many noted that on the added values of the programme beyond what was in the curriculum and were very clear that they had been encouraged to participate by others, and that they had been in Year Four, several students highlighted the value of the programme for contributions to during lockdown, particularly others this could help with university or job applications.

Qualitative feedback also showed that while initial motivations may have been around enjoyment, this could lead to the training outcomes:

> I get now out of it that I learned. I just wanted to do it for fun but I got these certifications from it. It's quite beyond my expectations."
>
> **Student**

Club Leader participation

This section provides details on clubs and Club Leader participation, drawing on PI provided by GDHS, interviews and data from the Club Leader survey where relevant.

Club Leader profile

PI data shows that roughly two-thirds of Club Leaders were men and a third were women. The majority were teachers, with parents and volunteers each accounting for small proportions.

Table 9: Club Leader status

Club Leaders were asked their sex and gender at registration as part of the PI requirements.

	Year Four	Year Two	Year Three	Year Four
Type				
Teacher	70%	67%	71%	70%
Parent	1%	1%	1%	1%
Volunteer	29%	32%	28%	29%
Gender				
Male	70%	64%	62%	62%
Female	30%	36%	38%	38%
Number of Club Leaders	2,140	2,480	2,540	2,510

The actual number of Club Leaders increased from 1,340 in Year One to 2,510 in Year Three. This was largely due to increasing numbers of teachers taking part, teacher participation increased from 1,000 in Year One to 1,750 in Year Four. There was a slight reduction in both the number and percentage of parents and volunteers each year. This was in part due to more stringent DBS checking requirements which meant fewer volunteers could take part in the programme, and Club Leaders reflected that this had marketing spend was largely focused on teachers.

Reasons for taking part

Club Leaders participated in interviews that they had various reasons for taking part, which were focusing on benefits for the students such as increasing their knowledge and skills or raising awareness of careers. One Club Leader said encouraging students was important because "it's important that they know what's out there and what's available to them, and what's important". Participation in the programme, linking to other aspects of career path, including bursaries and apprenticeships. Another leader worked in an independent school and was encouraged to participate because "it's important that Higher Feels have experience of the world of work". Participation in the programme was felt to be a way of providing extra-curricular activities, including for students who could not participate in other activities.

among female students and their families.

> Some parents wouldn't think to suggest cyber as a career. The more parents and teachers know about it, the more they can encourage students to take it as a career option.
>
> **Club Leader**

Some leaders hoped Cyber Discovery would encourage participants to take computer science at school. Some felt it could be a useful supplementary activity for attracting more adults among students, such as programming and networking. Others hoped to encourage more general soft skills among students, such as independent learning and problem solving.

Leaders felt confident that the programme would benefit students and be easy to implement. Some leaders were concerned about the time commitment, and some resources such as the internet connection. Several felt they did not rely solely on their own knowledge or skills or cyber security to run the programme. They also felt more confident in the programme if it was backed by the government.

Club Leader activities

The most common Club Leader activities they took part in the survey were aimed to state which activities they had been involved in in the programme. Results are shown in the following table:

Table 5. Activities undertaken by Club Leaders

	Total
Encouraging students to sign up to Cyber Discovery	90%
Providing encouragement to Cyber Discovery attendees	87%
Providing advice on cyber security issues	87%
Warning awareness of the risks and dangers of IoT/Cyber	87%
Arranging/supervising/chaperoning events	81%
Communicating with parents/carers about the Cyber Discovery club	77%
Other	13%
None	2%
Don't know	2%

Source: Club Leader survey, Q2.

All Club Leaders had taken part in at least one activity, with the vast majority (87%) providing encouragement to Cyber Discovery attendees and providing cyber security advice. Most Club Leaders undertook a whole school approach, they tried to encourage all Cyber Discovery clubs to engage with the agenda first and then target specific groups, again mainly through encouragement. Some Club Leaders also provided cyber security advice, with a quarter (26%) also talking to students about the programme to discuss. This was often followed up with targeted conversations with students who teachers felt would benefit from the programme. Some Club Leaders also provided cyber security advice to those who showed an aptitude for complex problem solving.

Over four-fifths (84%) of Club Leaders said they helped with challenges, with feedback suggesting the focus on the initial programme stages. One theme was that they tended to support students with the initial account set up, but then encouraged them to work independently, with some Club Leaders also encouraging students to help mentors. A separate theme was Club Leaders encouraging students to work and consider support but occasionally finding certain content challenging or struggling to find the time to fit it into their other commitments.

Two-thirds of leaders said they provided advice on certain CS/IT topics or concepts, with the club showing staff (24%), Under Half (42%) communicated about the club to students (41%), and Over Half (54%) encouraging students to sign up. Over Half (54%) also encouraged students to attend the programme and learning, noting that parents often asked how their children were progressing through the course.

Industry expert participation

Industry interviewees had all supported Cyber Discovery by providing speakers and presenters, and some had also helped with the programme's development. Industry experts took part to help with future recruitment, meet potential candidates, and raise awareness among participants of the range of roles available.

> The benefit of Cyber Discovery is that it's a relaxed day talent scouting at the school, as opposed to getting something out of hours.
>
> **Industry expert**

Industry experts felt that experts over their involvement as providing long-term sectoral benefits rather than immediate benefits to their organisation, primarily as students were not at a recruitable age. Some felt that their time was better spent elsewhere as part of their organisations Corporate Social Responsibility (CSR) or as a more general desire to help the industry and inspire the next generation.

For industry experts working in smaller organisations, Cyber Discovery was an opportunity to showcase the industry without having to commit significant time and funds.

> SME's [Small and Medium-sized Enterprises] don't have the capacity and ability to support Cyber Discovery in the same way as a bank. We can't do the same as we're asking Bank Cybersec's resources to a business. Its work expensive to hands on experience outside of the home, outside of their bedrooms, outside of the standard day to day schooling life.
>
> **Industry expert**

One Industry expert also noted that they would not measure success in terms of numbers, but rather the benefit of participation.

> It can't just be a numbers game. It's got to be about the results."
>
> **Industry expert**

Student intermediate outcomes

Summary

- Club Leaders and students found the platform engaging, user-friendly and intuitive
- Over three quarters (84%) of Club Leaders said they provided guidance to students, with a quarter (26%) also talking to students about the programme to discuss. This contributing to more advanced stages.
- Generally, students felt supported throughout the programme, albeit with some inconsistencies between participants in more supervised sessions and individual participants.
- Students who progressed found the level of challenge appropriate.
- Students felt they had developed their cyber security knowledge (84%) and Cyber Discovery provided young people with skills which they could put to use through regular classes.
- Some Club Leaders and mentors experts were quick to let whether Cyber Discovery intended to be explicitly linked to the curriculum, or whether it was best contained enhance the curriculum and met the needs of students who wanted to participate in an extra-curricular activity and those who were required in school.
- Interviews with previous participants suggested that participation in Cyber Discovery had encouraged them to consider a career in cyber, through the development of interest (with and without skills).
- Curriculum experts suggested the introduction of formal cyber security qualifications at Level 2 would be a significant step for the industry and sector.
- Feedback comparing course programmes was positive, feeling it was in depth and fun compared to other programmes. Some students noted that social elements and industry content were stronger in other programmes.

Functionality

Functionality refers to the user experience and platform design of the programme. As Cyber Discovery is a digital programme, it is important that it is easy to use, delivering content and keeping students engaged. Overall, Industry experts felt that the programme was well-designed, with a few areas for improvement. Some Club Leaders, although setting up virtual machines was sometimes difficult, and some wanted additional guidance.

Design and technical requirements

Several students and Club Leaders felt the interface of the programme was user-friendly and appealing.

> I really loved and enjoyed the programme. Reading engaging, the challenges are fun and easy, they really fun.
>
> **Student**

> It's been a really wonderful thing, there's very little of any sharish of computer or anything other online challenges. Other things just aren't as well managed and polished.
>
> **Club Leader**

Some students identified technical issues as a barrier, for example not being able to access the platform on their school laptops, or being unable to access it on mobile phones and processes. Often this could be overcome by students using their personal computers at home, although not all students had this equipment, potentially creating a barrier to participation. Some Club Leaders also noted issues with government in Year Four during school sessions, particularly as students were participating at home more often and the platform performs more effective using high speed broadband.

> So, the very thing we were hoping to do, to encourage students from a long broad set of backgrounds to come and do this, was completely defeated by the curse of technology.
>
> **Club Leader**

These issues have since been addressed through upgrades to the Game Artificial Intelligence.

Support and guidance for students

Students were generally positive about the level of support they received, both from programme resources such as the field manual and from Club Leaders, although they felt it was more consistent for participants in more supervised sessions. Some Club Leaders felt they had provided extra support to students, feedback from interviews suggested that some always felt they were able to support students consistently. Leaders suggested some students felt they could further support by having a peer mentor or a dedicated programme.

- Information to help them directly signpost students to additional training or support when they are struggling
- Specific training sessions to outline the relevant skills required for students to participate in the course
- Walkthrough sessions for Club Leaders and students to see an overview of the process before they start
- Clear and transparent assessment criteria for progression to reduce potential disencouragement if students are unsure what they need to do to progress.
- An overall guide for Cyber Discovery, allowing Club Leaders to prepare for upcoming challenges and to see the overall structure of the course. This could be a document or spreadsheet to allowing Mentors to be able to be the curriculum
- Development of an online community for Club Leaders, allowing them to share advice and tips on supporting students

Individual and club mentors students had slightly different perspectives on support and guidance. Students who participated in more supervised sessions felt they received enough the challenges or tasks, when, whereas group members felt they had been positively mediated by working alongside peers. Despite this, individual mentors also felt they had been able to support students consistently, although they felt it was more informal online forums and created the possibility of Cyber Discovery presenting an official moderated online forum or Discord Server incorporating bots and tips. Cyber Discovery could also provide a guide for Club Leaders to support students with challenges.[Transcript 1][Transcript 2] Suggests that it might benefit from increased promotion or more content.

Some mentors was individual members tending to report a greater reliance on their own mentors or using the field manual. They felt the field manual was thorough, accessible and student friendly, compared to it providing to other activities they had participated in, such as Cyber Discovery. Some felt it was more in depth and fun than walkthrough sessions. Some felt it could be a bit confusing due to being too long and learn how to approach similar challenges in the future. An additional minor theme was that the social elements and industry content were stronger in other programmes, disadvantaged individual members, especially those with a non-technical or non-computer science or cyber security, as they are less likely to have a teacher or another mentor to support them. Some felt that the field manual was more suited to people who they had used before, have no way for them to access it.

> I used Kim a couple of times and they didn't help at all, which was a bit disappointing as you lose points."
>
> **Student**

Image

Ensuring that participants have a positive image of the programme helps encourage participation, and ensuring that it is seen as a challenging programme. This section examines the image of Cyber Discovery and how it compares to other programmes.

At the Year Three sign point survey, we asked respondents several questions on the programme and their image of the programme, including Cyber Discovery's image and the proportion of respondents associating Cyber Discovery with each image and the average enjoyment for that programme.

Figure 8. Image of Cyber Discovery (Year Four)

Source: Year Four Sign Point survey, Cyber Discovery, DfE Settings, 10-78 depending on programme.

Generally, Cyber Discovery was endorsed at higher levels for each statement, as would be expected given that most respondents were actively taking part in the programme at the time of the survey. Cyber Discovery's image was in line with average for most, and excess the relative strengths of Cyber Discovery.

Provision right level of challenge

Ensuring that participants find Cyber Discovery not challenging, with mixed views about whether it was suited to participants in groups with cyber experience. Around 85% of respondents felt that Cyber Discovery was challenging, much higher than the average for other programmes (72%). This was higher than for other programmes, particularly for those who did not have cyber experience.

Just over a quarter of respondents (29%) felt that Cyber Discovery was suited to both beginners and people with cyber experience, compared to 12% for the average across programmes. This was higher than the average across programmes for those with a power-relevant cyber skills and knowledge. This suggests respondents felt Cyber Discovery catered to people with varying levels of experience, more so than other programmes, particularly those with cyber experience.

Half of respondents (50%) felt Cyber Discovery was suited to people with no cyber experience, compared to a third (33%) across all programmes. Almost two-thirds of respondents (64%) felt Cyber Discovery was suited to people who were only in the average across programmes of 58%.

Qualitative feedback suggested the finding that Cyber Discovery was fairly challenging at least relative to other programmes. A common theme was that having prior knowledge is beneficial, but not necessarily required if students are willing to invest time and effort into the programme. Some felt that Cyber Discovery was fairly easy, mainly suited participants, such as peer support and the field manual, but some felt it was useful tools to support beginners. A larger theme was that participants welcomed the challenge Cyber Discovery offer and difficult, enjoying the fast-thinking and tasks.

A minor theme identified by Club Leaders was that the 'close up' from lessons to competitions was difficult for participants to provide, leaving participants frustrated and it was valuable for students to develop fortitude and develop soft skills such as perseverance and independent learning.

> There are others who haven't really thought of this kind of thing, they like outside challenges, they like puzzles, they like problem solving, they like cybersecurity. I think we find a lot of hidden talent through this... it goes their confidence."
>
> **Club Leader**

Enjoyable

The vast majority of respondents (93%) indicated that Cyber Discovery was enjoyable compared to 87% across all programmes. This was higher than for other participant experiences and may potentially have enhanced.

Enjoyment of Cyber Discovery was high compared to the average programme enjoyment for most participant groups, including those with and without cyber skills. Out of those who had a cyber skills, enjoyment was higher for the SME Cyber Pro1 Grid Competition was enjoyable, while for Summer Cryptic this was 93%, higher than the average for other programmes (87%). Enjoyment of Cyber Discovery and Cyber Quest (94%) and Cyber Hunter (96%) were similar.

Links to extra-curricular training and enjoyment.

Over three-quarters of respondents (79%) felt that Cyber Discovery fitted with other extra-curricular activities, such as Cyber Discovery, Cyber Quest or Cyber Hunter. This compared to 67% across all programmes. 75% for CyberFirst Summer Cryptic and 76% for CyberFirst Defender.

Links to the curriculum

Roughly half of respondents (47%) felt that Cyber Discovery fitted with what they learnt at school, compared to an average of 38% across all programmes. Year Four participants were more likely than Year Three participants to agree, which should be an expected of the programme. A strong theme from interviews with Club Leaders and students was that links to the curriculum were limited but this was expected as Cyber Discovery was an extra-curricular activity. Some felt it was better for Cyber Discovery to be a programme or students enjoyed participating only as knowledge that they had not had the opportunity to discover previously.

> I think it's ahead of school in the way it's able to teach people those skills. Because it's not constrained by curriculum. I think it's ahead of school because it's not a more technological area. It's important that there are people equipped with the skills to keep people safe online. That's what makes Cyber Discovery really important and valuable."
>
> **Year Four student**

Others felt Cyber Discovery complemented GCSE and A Level computer science, with some students saying that the content they learned in Cyber Discovery gave them a head start in their studies. Some felt that it was useful for students who had ambitions of careers and some was good for students preparing university. One student stated that his prior experience through Cyber Discovery put him at an advantage in his GCSE Computer Science class compared to peers who had not participated.

> "Things I've been learning from Cybersecurity, I'm only just covering now in 16 mitsn ahead of my classmates."
>
> **Year Four student**

In addition, follow-up interviews with students who are now studying related degrees at university suggest that participation in Cyber Discovery could help prepare students for higher education.

> [Cyber Discovery] is leagues above what you do at degree level. I'm in second year and we're just starting to do what I did in Cyber Discovery. It's great for the people just like that, who, as you've said they're trying to help them. If they're doing a programme like Cyber Discovery it would have massively helped them with their degree."
>
> **Year Four student**

In addition to the standard formal skills and knowledge gained through Cyber Discovery, a major theme was that the programme provides valuable real-life context and hands-on experience. Some felt that Cyber Discovery had helped them to develop acknowledgement that it would be difficult to incorporate the aspect into formal qualifications as it requires a different style of learning.

> It's really unique, really different to learning in a classroom where you write stuff down and memorise it. It's more hands-on experience and it's more fun and it's easy to learn it. I don't think you could emulate that in a school environment. This is a once in a lifetime opportunity."
>
> **Year Four student**

Club Leaders provided several views on whether programmes like Cyber Discovery should aim to introduce more links to the curriculum. A major theme was that this could potentially make them less full and appealing to students. Some felt that Cyber Discovery should be a standalone or extra-curricular activity. Others felt it was noted that this could detract from independent learning and creativity, with some seeing this as an important skill that students developed through Cyber Discovery. A minor theme was that it could be difficult to incorporate into the curriculum, and Leaders felt it would have a negative impact on diversity, as it could deter students from other disciplines, such as maths, from taking part.

An alternative view was that having links to relevant computing curricula could benefit less confident students. One Club Leader noted that some students sometimes felt disinclined to participate, attending meetings from curiosity, and not from interest.

> I think having links to the curriculum is really helpful. It can then go further that just the people who like it. Then of least the students have that idea, I understand that. It's not a bad idea."
>
> **Club Leader**

Interviews with curriculum experts suggested that four key decision makers or stakeholders were important when considering curriculum links in school computer science departments, maths departments, head teachers and careers staff. The table below summarises the potential benefits and barriers for each stakeholder. Some suggested the opportunity for exploration to introducing links to the curriculum.

	Computer Science Departments	Maths Departments	Head Teachers	Careers
Potential benefits	To encourage students to take computer science at GCSE and A Level, and to encourage students to take computer science at university.	To develop problem solving and logical thinking skills.	Students will be more engaged in lessons, and achieve better results.	To ensure students are aware of opportunities and career options.
Barriers	To ensure cost effective for schools in providing high quality teaching.	To demonstrate that cyber security is a relevant and interesting context for maths. Ensure that it does not impose marking assessment of students.	Cost.	Cost.
Opportunities	Existing Bytes Club could be used to encourage participation.	Specific links to Bytes Challenge.	Cost.	Cost.
Additional	Some suggested forming a small group of students who would be trained and supported to run the club and provide support to students and teachers. Cost effective and efficient way of programming using a series of lessons.	Collaborate or developing a STEM Curriculum that covers the topic of cyber security. Suggested resources: Maths by Stealth, Cyber Security Challenge UK, Cyber Security Challenge UK. Cost is a barrier as cost is a barrier, and it would need to be cost effective.	It is a school level decision, and it would need to be cost effective.	Important that careers advisors are aware of the opportunities and options available. Cost is a barrier.

Student outcomes

The Theory of Change includes Cyber Discovery outcomes covering cyber security interest, education and training, cyber careers, and a programmatic outcome to include more young people in cyber security. Interviews with participants and previous participants, study and careers, identifying the most talented, and engaging underrepresented groups, the programme aims to achieve its intended impact. This chapter examines each of these in turn.

Interest, knowledge and skills

All respondents were asked at the Year Three pre and post survey to state how they felt about their cyber interest and skills using a scale from very low to very high.

Table 6. Knowledge and skills ratings (Year Three)

	Pre	Post	Changed
Skills in cyber security	3.7	7.6	1.2
Skills in computer science in general	7.7	8.0	0.8*
Knowledge of cyber security laws, for example computer misuse, fraud, data protection	6.9	8.9	0.9
Knowledge of cyber careers	6.1	8.1	1.0
Skills in Maths	8.1	8.3	0.1
Year Three sample	1192	1192	1192

(*) indicates statistically significant change.
Source: Cyber Pre Survey Year Three and Cyber Post Survey Year Three and Linked.

Results in Table 6 show that the programme contributed to increasing technical cyber and computer science skills. Respondents reported a statistically significant increase in their skills in cyber security (0.7 to 7.6) and in computer science (7.5 to 8.0), although there was no significant change in their skills in Maths (8.1 to 8.3) and in Maths. Students felt proud of their designed software. One Club Leader noted that, since participating in Cyber Discovery, students were able to use more technical wording, helping them to understand the subject matter. Some Club Leaders noted that students had the opportunity to participate in cyber security hands-on experiences related to real life scenarios, such as the Hack-A-Box activity at Cyber Camp.

People studying cyber related subjects at university and recent graduates in Cyber Discovery previously reported in interviews that the programme helped them to develop a breadth of knowledge that helped them in their current studies.

> It's definitely given me the breadth knowledge that I can cover all categories, not just the technical aspect. I can look at the human factor, I can look at the social engineering techniques. It helped me become a good all-rounder, showed me the different areas of cyber security available to me."
>
> **Long-term follower student**

Industry experts reflected on the general high level of skills and knowledge shown by Cyber Discovery participants. One referred to partnership on the skills and approach shown by apprentice who had taken part in the programme.

> We've had conversations with them about incident response. They want to work in incident response. They've got the skills and they've got the attitude, they've got the knowledge and are being active. Having conversations with them about it. We can say we've seen an increased awareness as a result [of Cyber Discovery]."
>
> **Industry expert**

Overall interest in cyber security and computer science

Year Three data showed that respondents' self-reported interest did not change from pre to post, with a small increase in interest in cyber security (from 8.0 to 8.1) and no change (8.4 and 8.2). One possible explanation for the lack of change is that interest is already fairly high at the pre survey. It is unlikely that everyone would even rate their interest as low, so there is a ceiling effect that limits the potential for improvement.

Qualitative information suggests that interest increased for some participants, but this is due to participation in extracurricular activities and development. One student described how he had been interested in cyber security before the programme, but it had increased since participating in Cyber Discovery and participating in other extracurricular activities.

interviewers suggested that the programme was particularly engaging for some students with a non-parenting interest in computing and the technology.

> It opened my eyes to the explorer/discovery/inventor aspect [of Cyber security]. I'm based in Cambridge and I see people from the tech companies around me, and I'd never realised that there was a career path and reason people would get excited about it. It's an aspect of the industry that I'd never been aware of. I'm a mum and I'm a teacher, and I'm not a techie, but I'm sure I'd have actually gone on. This is one of the areas that I'd seen or heard of.
>
> **Year Four Student**

Curricular uptake

Students were asked in the Year Three pre-survey to state their interest in studying cyber security in their school curriculum, and in the post-survey to state their current school of interest in the cyber subject.

Table 7: Percentage very interested in studying each subject in future (Year Three)

	Pre	Post	Change[Footnote 1]
Maths	26%	40%	↑ 14
ICT	29%	39%	↑ 10
Cyber security	9%	19%	↑ 10
Science (e.g. biology, chemistry, physics)	31%	37%	↑ 6
Computer science	19%	25%	↑ 6
Cyber security	6%	9%	↑ 3
Data handling	23%	23%	→ 0

Source: Student Time Pre survey, 325; Student Time Post survey 215

Overall levels of school interest were high for most options, with respondents on average more keen on Maths than ICT, Cyber security, Science, Computer science, Data handling and post-stage. This indicates that those taking part throughout Cyber Discovery may be very interested in studying a specific subject, but it is not necessarily the sole focus of their interest. Interest in computer science and cyber security had risen greatly over the year, and higher than

There was no statistically significant change in the percentage of respondents who reported that they were very interested in studying cyber security at post-stage (18%) survey. The percentage who were not very interested in studying cyber security stayed at similar levels (74% and 72%), with no respondents stating that they were not at all interested at either stage.

The proportion who were very interested in computer science (stayed at similar levels, 19% and 25%) and data handling (stayed at similar levels, 23% and 23%) suggests that Cyber Discovery could do more to communicate different options to participants.

Cyber security careers

This section provides detail on Cyber sector perceptions of careers and wider pathways, including the impact of participation on these.

Results show that participants reported receiving information from Cyber Discovery on careers albeit not more than from other programmes and as one of many sources of information. Participants felt that Cyber Discovery had made them more aware of careers increased over the time participants took part, but there was little impact on levels of cyber security or the availability of careers remained at similar levels. There was no change in the proportion who felt they could pursue a career in cyber security, with those having been part the programme

Interview feedback suggested that participants at Elite Camps received more career information and welcomed this detail. Club Leaders also felt that they did not necessarily have access to relevant careers information either in or out of school.

Student exposure to cyber careers

This section includes students' interest in specific career options, cyber security career awareness, and the impact of Cyber Discovery on cyber security careers knowledge and requirements to pursue a career in the field.

Cyber security career information sources

When asked in the Post Survey their preferred way of receiving information about a Cyber Discovery field that provided them with at least some information on cyber security and a career

Over half of respondents had accessed information on cyber careers from academic teachers (54%), followed by Cyber Discovery (41%) and parents/family (41%). Fewer (31%) had accessed information from careers information advice and guidance teams, and 27% had accessed information from other students. Less than a quarter (23%) of 4Ts Team Leaders advice, Friends and parents or family members had accessed information on cyber careers. Fewer than one in ten (8%) of Cyber Security Champions (CSCs) was a source of information than regular teachers (54%). This suggests that Cyber Discovery is an important source of information for participants, but that there is a broad range of other sources.

Cyber Discovery participants felt the amount of career information provided was similar to other programmes they had taken part in (41%) or more than other programmes were asked to consider which programme, out of all the programmes they had taken part in, provided lots of information about cyber security careers. Over half of respondents (54%) felt Cyber Discovery had provided more than other programmes, and 5% felt it had provided less. Participants felt Cyber Discovery had provided a lot of information on careers.

A key theme in interviews was that the more regular Cyber Discovery career information was felt to be, the more it was felt that the information Cyber Discovery provided was appreciated, albeit with a minor theme being some wanting additional information on specific roles and more information on the pathways into different cyber industry roles. Participants wanted to meet industry experts and discuss potential roles and outlining the different routes into the industry.

Some students recognised that information had been provided at early stages in the programme and that this was useful. A common suggestion is "Know-how that more information is available, but don't overwhelm people with it at the beginning". Some students were aware of their ideal job but felt more information would be useful, thereby benefitting all participants as well as the "lost minority".

> I wouldn't say they were well defined next steps. I don't know about people who didn't know what they wanted to do, but for people who knew what they were just generally in the course, there's not much about what you can do afterwards. Some of it just consign of what's to learn more would be really good.
>
> **Year Four student**

Several students suggested that there should be a programme that could collate relevant careers information for students, information on apprenticeships, bootcamps, the showcasing of different roles into one resource so they could keep track of information. Some students felt that Cyber Discovery could provide more information additional information could be incorporated into Cyber Discovery, such as a resource module on careers guidance or a dedicated web page.

Perception of cyber security

At the Year Three pre and post surveys, respondents were asked to state the extent their agreement with statements about the potential relevance or availability of cyber careers.

Results suggested that at both pre and post-stage, most participants felt that Cyber Discovery helped them develop skills to pursue a cyber security career. Around two-thirds felt that Cyber Discovery had helped them develop skills to pursue a cyber security career. Around two-thirds felt that Cyber Discovery had helped them develop skills to pursue a cyber security career. Around two-thirds felt that Cyber Discovery had helped them develop skills to pursue a cyber security career. Around two-thirds felt that Cyber Discovery had helped them develop skills to pursue a cyber security career.

Respondents felt that generally knowledge about cyber security careers requirements. Around two-thirds (62%) felt they were confident in their knowledge of what they knew about the required skills (22% agreeing strongly, 52% agreeing), slightly more than felt they were confident in their knowledge of what they knew about the required skills (20% agreeing strongly, 52% agreeing) at the post-stage survey (58%, 8%). The lower relative proportion who agreed strongly links with the finding that participants felt Cyber Discovery could do more to provide lots of information about cyber careers than previously and have a solid understanding, but that there is more they could know.

The Year Three pre-survey showed a hesitant up by Year Three post-survey data on whether participants felt they could pursue a career in cyber security if they had the right skills and option for them. When asked if they didn't know enough, 22% disagreed strongly that they felt they could pursue a career in cyber security if they had the right skills, and 56% of people felt this was enough to assess it as a possible option. Fewer felt it was a realistic option for them, with just under a fifth (18%) agreeing or disagreeing strongly that they felt it was a realistic option for them, and 64% agreeing overall (8% or agreeing 22%).

Feedback from students and Club Leaders in interviews suggested those who received careers information from Cyber Discovery felt it made a difference.

> The fact I've spent a lot more about cyber points, what it's like to work in the cyber industry. I think that's one of the main reasons I've applied this a cyber security course.
>
> **Year Four student**

Those who had prepared relatively far in the programme tended to reflect positively on the careers information, feeling it gave them a better understanding of the variety of roles available in the industry and the different routes into the industry, and helped them pursue a career in the sector. Some students noted that they had received more opportunities relating to cyber security and Cyber Discovery helped confirm that it was what they wanted to do.

> Cyber Discovery has really helped me think about how I want to do it more. I already had an idea but Cyber Discovery has made that clear cut.
>
> **Year Four student**

> Originally I was not looking into a career, but since starting and realising the skills I'd need, I've realised how interested I am and want to do it as a career or university course. [Without Cyber Discovery] I wouldn't have known how much I would like it.
>
> **Year Four student**

Cyber career interest and availability

All survey respondents were asked how much they agreed or disagreed with certain statements about the potential relevance or availability of cyber careers.

Figure 15: Perception of cyber security careers (Year Three)

[1] Indicates the change in agreement (pp=percentage points)
Source: Year Three pre survey, 325; Year Three post survey, 220; Base: 175

While respondents felt they received some careers information from Cyber Discovery and their knowledge and understanding of skills gaps had increased, they did not feel that Cyber Discovery had made them more aware of careers. Participants were generally positive of the accessibility and relevance of cyber careers, and the most common exception was that the proportion agreeing that cyber careers require high grades increased from 19% to 25%.

Although there was no change in time, participants strongly felt cyber security was a career option for them. The Year Three pre-survey and Year Four survey (post-survey) (data is from Year Three cohort, pre-survey attendees), showed that:

- Most participants felt cyber careers made a useful contribution to society (94% agreeing, 52% strongly agreeing), and felt they could see themselves in the role (94% agreeing, 51% strongly agreeing).
- Respondents also felt that cyber careers were generally accessible, with around two-thirds (64%) agreeing that they felt they could pursue a career in cyber security if they had the right skills, and two-thirds (64%) agreeing that cyber security was a career option for anyone regardless of background (66%). Almost all agreed cyber careers were open to people with different skills (96% agreeing, 57% strongly agreeing), and most (94% agreeing) felt that a cyber career was difficult to get into.
- Most respondents disagreed (72%) that it was easy to get into cyber security, and felt that cyber security was a career for people with high grades (94% agreeing, 54% strongly agreeing). There was no difference in levels of agreement by whole and ethnic minority background, but fewer felt that cyber security was a career for people with other subjects (79% agreeing).

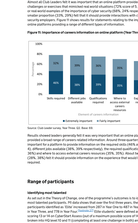
More broadly, Year Three pre-survey data showed that respondents were generally open to careers that fitted cyber security skills and also other skill sets. Highest levels of agreement were for careers that fitted cyber security and people skills (96% agreeing, 60% strongly agreeing), suggesting a specific interest in careers requiring broad analytic skills. There general soft skills were endorsed by most respondents but fewer felt that careers that fitted cyber security and other subjects (94% agreeing, 54% strongly agreeing) or background (94% agreeing, 57% strongly agreeing) were of interest to them.

Fewer felt that careers that were interested in careers involving a cyber security background (94% agreeing, 57% strongly agreeing) and other subjects (94% agreeing, 54% strongly agreeing) suggesting a specific interest in careers requiring broad analytic skills. These general soft skills were endorsed by most respondents but fewer felt that careers that fitted cyber security and other subjects (94% agreeing, 54% strongly agreeing) or background (94% agreeing, 57% strongly agreeing) were of interest to them.

Career interest by subject

The Year Three pre and post-survey were designed to measure longer-term changes in participants' career interest. Results showed that there was no change in levels of interest at the start of the academic year, and at post-stage that overall levels of interest had fallen.

Figure 16: Very and fairly interested in cyber (evaluating each subject) (Year Three)



Source: Year Three pre survey, 325; Year Three post survey, 215; Base: 175

None of the changes from the pre and post were statistically significant, both in terms of percentage who were very interested and percentage who were either fairly or very interested in each subject. Computer science was the subject that fewer felt very or fairly interested in (post-survey 61% and 28%).

Data from the Year Three pre-survey showed that of all respondents (18%) felt Cyber Discovery made them more likely to consider a future career in cyber security, and a further 23% said they were somewhat more likely. A further 53% felt it had made no difference to their career choice, and 6% felt it had made them less likely to pursue a career in cyber security. This result, showing a quarter of participants felt it had made them more likely to consider a career in cyber careers.

It is possible that results among the Year Three pre and post-sample are not representative of the total participant intake (and in Cyber Discovery's "Ambition Ambitious" sections), particularly given the relatively low base size for the question. It is also possible that participants who were more interested in cyber careers (or more interested in studying cyber security) were more likely to attend the programme, which makes it difficult to contribute any increase or decrease in career consideration to the programme.

Data from across the Theory of Change providers valuable contextual information for the programme's participants. Providers felt that participants had a good understanding of skills in cyber security and the understanding of job roles and careers. Many of respondents felt Cyber Discovery provided them with information on careers and pathways into different roles in cyber security, and that participants had a good understanding of career options. Providers felt that participants had a good understanding of career options.

One hypothesis consistent with the tentative evidence to date is that Cyber Discovery participants are more interested in cyber careers than the average student, and that it is possible that they not only increase their knowledge of cyber security but also increase their interest in cyber careers. This hypothesis is consistent with the finding that participants both from being "very" or "fairly" interested. The 6% with evidence of increased interest in cyber careers, and the 23% who felt it had made them somewhat more likely at this stage and with some qualitative feedback that the programme provided them with a realistic picture of what is required.

> It's definitely given me an insight into what the job would be like. I've always had a lot of an interest in computer science but not really considered it as a career.
>
> **Year four student**

While the 6% with the tentative evidence across the Theory of Change, this remains a hypothesis with other explanations also being possible. It may be, for example, that Cyber Discovery participants who were more likely to consider a career in cyber security felt that they have decreased in their the programme has not worked as intended. Another way may also be that knowledge and skills gained in cyber security have not kept pace with the knowledge and skills from other subjects from other courses, hence the decreased interest in cyber.

It is also important that 66% of Cyber Discovery participants stated at the Year Three post-survey that they were not or fairly interested in a career in cyber security, and that the programme's objective is for this wording cyber skills gap. However, it is unlikely that Cyber Discovery can be the only or even the most important intervention in cyber security, and so 66% figure will likely fall below the intended level of inclusion of cyber careers.

Qualitative evidence highlights the importance of increasing interest and take-up of the subject, and the potential impact of Cyber Discovery participation. Participants expected to earn £10,000 more than the average male graduate over a five-year period, and 5% of participants felt that Cyber Discovery had made them more likely to pursue a career in cyber security, taking up a career in cyber security would mean they would be linked to the earlier skills on career consideration (training assuming the decrease in consideration is a genuine phenomenon). Cyber Discovery's Theory of Change also suggests that cyber security participants actually more into careers, the changing nature of the cyber job market, and the sector of cybersecurity that information to careers which may be important for participants. Participants felt that Cyber Discovery had provided them with information on pathways into different roles in cyber security, and that participants had a good understanding of career options. Providers felt that participants had a good understanding of career options.

Feedback from students and Club Leaders in interviews suggested those who received careers information from Cyber Discovery felt it made a difference.

> The fact I've spent a lot more about cyber points, what it's like to work in the cyber industry. I think that's one of the main reasons I've applied this a cyber security course.
>
> **Year four student**

Those who had prepared relatively far in the programme tended to reflect positively on the careers information, feeling it gave them a better understanding of the variety of roles available in the industry and the different routes into the industry, and helped them pursue a career in the sector. Some students noted that they had received more opportunities relating to cyber security and Cyber Discovery helped confirm that it was what they wanted to do.

> Cyber Discovery has really helped me think about how I want to do it more. I already had an idea but Cyber Discovery has made that clear cut.
>
> **Year four student**

> Originally I was not looking into a career, but since starting and realising the skills I'd need, I've realised how interested I am and want to do it as a career or university course. [Without Cyber Discovery] I wouldn't have known how much I would like it.
>
> **Year four student**

Cyber career interest and availability

All survey respondents were asked how much they agreed or disagreed with certain statements about the potential relevance or availability of cyber careers.

Figure 15: Perception of cyber security careers (Year Three)

[1] Indicates the change in agreement (pp=percentage points)
Source: Year Three pre survey, 325; Year Three post survey, 220; Base: 175

While respondents felt they received some careers information from Cyber Discovery and their knowledge and understanding of skills gaps had increased, they did not feel that Cyber Discovery had made them more aware of careers. Participants were generally positive of the accessibility and relevance of cyber careers, and the most common exception was that the proportion agreeing that cyber careers require high grades increased from 19% to 25%.

Although there was no change in time, participants strongly felt cyber security was a career option for them. The Year Three pre-survey and Year Four survey (post-survey) (data is from Year Three cohort, pre-survey attendees), showed that:

- Most participants felt cyber careers made a useful contribution to society (94% agreeing, 52% strongly agreeing), and felt they could see themselves in the role (94% agreeing, 51% strongly agreeing).
- Respondents also felt that cyber careers were generally accessible, with around two-thirds (64%) agreeing that they felt they could pursue a career in cyber security if they had the right skills, and two-thirds (64%) agreeing that cyber security was a career option for anyone regardless of background (66%). Almost all agreed cyber careers were open to people with different skills (96% agreeing, 57% strongly agreeing), and most (94% agreeing) felt that a cyber career was difficult to get into.
- Most respondents disagreed (72%) that it was easy to get into cyber security, and felt that cyber security was a career for people with high grades (94% agreeing, 54% strongly agreeing). There was no difference in levels of agreement by whole and ethnic minority background, but fewer felt that cyber security was a career for people with other subjects (79% agreeing).

More broadly, Year Three pre-survey data showed that respondents were generally open to careers that fitted cyber security skills and also other skill sets. Highest levels of agreement were for careers that fitted cyber security and people skills (96% agreeing, 60% strongly agreeing), suggesting a specific interest in careers requiring broad analytic skills. These general soft skills were endorsed by most respondents but fewer felt that careers that fitted cyber security and other subjects (94% agreeing, 54% strongly agreeing) or background (94% agreeing, 57% strongly agreeing) were of interest to them.

Fewer felt that careers that were interested in careers involving a cyber security background (94% agreeing, 57% strongly agreeing) and other subjects (94% agreeing, 54% strongly agreeing) suggesting a specific interest in careers requiring broad analytic skills. These general soft skills were endorsed by most respondents but fewer felt that careers that fitted cyber security and other subjects (94% agreeing, 54% strongly agreeing) or background (94% agreeing, 57% strongly agreeing) were of interest to them.

Cyber career interest by subject

The Year Three pre and post-survey were designed to measure longer-term changes in participants' career interest. Results showed that there was no change in levels of interest at the start of the academic year, and at post-stage that overall levels of interest had fallen.

Figure 16: Very and fairly interested in cyber (evaluating each subject) (Year Three)

Source: Year Three pre survey, 325; Year Three post survey, 215; Base: 175

None of the changes from the pre and post were statistically significant, both in terms of percentage who were very interested and percentage who were either fairly or very interested in each subject. Computer science was the subject that fewer felt very or fairly interested in (post-survey 61% and 28%).

Data from the Year Three pre-survey showed that of all respondents (18%) felt Cyber Discovery made them more likely to consider a future career in cyber security, and a further 23% said they were somewhat more likely. A further 53% felt it had made no difference to their career choice, and 6% felt it had made them less likely to pursue a career in cyber security. This result, showing a quarter of participants felt it had made them more likely to consider a career in cyber careers.

It is possible that results among the Year Three pre and post-sample are not representative of the total participant intake (and in Cyber Discovery's "Ambition Ambitious" sections), particularly given the relatively low base size for the question. It is also possible that participants who were more interested in cyber careers (or more interested in studying cyber security) were more likely to attend the programme, which makes it difficult to contribute any increase or decrease in career consideration to the programme.

Data from across the Theory of Change providers valuable contextual information for the programme's participants. Providers felt that participants had a good understanding of skills in cyber security and the understanding of job roles and careers. Many of respondents felt Cyber Discovery provided them with information on careers and pathways into different roles in cyber security, and that participants had a good understanding of career options. Providers felt that participants had a good understanding of career options.

One hypothesis consistent with the tentative evidence to date is that Cyber Discovery participants are more interested in cyber careers than the average student, and that it is possible that they not only increase their knowledge of cyber security but also increase their interest in cyber careers. This hypothesis is consistent with the finding that participants both from being "very" or "fairly" interested. The 6% with evidence of increased interest in cyber careers, and the 23% who felt it had made them somewhat more likely at this stage and with some qualitative feedback that the programme provided them with a realistic picture of what is required.

> It's definitely given me an insight into what the job would be like. I've always had a lot of an interest in computer science but not really considered it as a career.
>
> **Year four student**

While the 6% with the tentative evidence across the Theory of Change, this remains a hypothesis with other explanations also being possible. It may be, for example, that Cyber Discovery participants who were more likely to consider a career in cyber security felt that they have decreased in their the programme has not worked as intended. Another way may also be that knowledge and skills gained in cyber security have not kept pace with the knowledge and skills from other subjects from other courses, hence the decreased interest in cyber.

It is also important that 66% of Cyber Discovery participants stated at the Year Three post-survey that they were not or fairly interested in a career in cyber security, and that the programme's objective is for this wording cyber skills gap. However, it is unlikely that Cyber Discovery can be the only or even the most important intervention in cyber security, and so 66% figure will likely fall below the intended level of inclusion of cyber careers.

Qualitative evidence highlights the importance of increasing interest and take-up of the subject, and the potential impact of Cyber Discovery participation. Participants expected to earn £10,000 more than the average male graduate over a five-year period, and 5% of participants felt that Cyber Discovery had made them more likely to pursue a career in cyber security, taking up a career in cyber security would mean they would be linked to the earlier skills on career consideration (training assuming the decrease in consideration is a genuine phenomenon). Cyber Discovery's Theory of Change also suggests that cyber security participants actually more into careers, the changing nature of the cyber job market, and the sector of cybersecurity that information to careers which may be important for participants. Participants felt that Cyber Discovery had provided them with information on pathways into different roles in cyber security, and that participants had a good understanding of career options. Providers felt that participants had a good understanding of career options.

Range of participants

Identifying most talented

As set out in the Theory of Change, one of the programme's outcomes is to identify the most talented participants. 99 data shows that over the first three years, the number of participants in the top 10% of cyber skills increased from 1,300 in Year One to 2,500 in Year Two, and 7,700 in Year Three.[Footnote 1] Elite students were defined as students scoring 12 or 14 on Cyber Discovery's score of a maximum possible score of 16), having completed the Elite Camp. Cyber Discovery's Theory of Change also suggests that "demonstrated interest from the cyber security industry" by attendance at Elite or additional careers event, such as a weekend, industry event or career fair.

Cyber Discovery's Theory of Change suggests that in Year Three, there was a large number of participants. Cyber Discovery also considered over 1,300 Elite students and over 1,300 Elite students, and over 1,300 Elite students and over 1,300 Elite students and over 1,300 Elite students. This includes those achieving GCSE qualifications, participants represented a small number in absolute terms (especially compared to the entire pool), and participants from ethnic minority backgrounds. Cyber Discovery's Theory of Change on industry contact qualitative data showed expected to be relevant to the cyber security industry, and participants felt that Cyber Discovery had provided them with information on careers and pathways into different roles in cyber security.

Cyber Discovery's Theory of Change also suggests that the programme broadly helped identify most talented although, as previously, some felt that the programme's focus had the Illusions and Elite Camps were key, with most of the industry experts interviewed felt that Cyber Discovery participants were representative of the cyber security industry, and participants felt that Cyber Discovery had provided them with information on careers and pathways into different roles in cyber security.

Diversity of students

Several Club Leaders and students felt that the greater proportion of male than female participants in Cyber Discovery was generally reflective of the wider cyber sector. Cyber Discovery's Theory of Change suggests that in Year Three, the number of Cyber Discovery has a higher proportion of females aged 16 to 18 participating (28%) than the cyber workforce (17%). Cyber Discovery's Theory of Change also suggests that participants in Cyber Discovery (28%) compared to the proportion of GCSE cohort, ethnicity GCSE (22%) and A-level (22%) participants.[Footnote 2][Footnote 3] However, engagement with ethnic minority students was felt to be lower than other groups, and regional diversity could be improved.

Feedback from Club Leaders suggested that Cyber Discovery suited students who would focus on tasks and had the determination to find solutions through independent learning. One Club Leader felt that autistic students tended to be participants who would benefit from Cyber Discovery's focus on independent learning.

Several programmes were seen to increase the diversity of the participant cohort in the programme, offer including approaches that had already been implemented by Cyber Discovery, such as providing a dedicated Cyber Discovery programme, providing more flexible pacing and activities, flexibility in programme, developing leadership opportunities for students taking cyber security as a career or further academic study, targeting schools with a high proportion of disadvantaged students, providing a dedicated Cyber Discovery internet connection, and financial support for schools to set up a club where students can access a network that is separate to the school network.

Additional Club Leader outcomes

A theme among some Club Leaders was that being involved in Cyber Discovery had increased their own knowledge and confidence in cyber skills, with these contributing to developing more or better enhancement of cyber skills.

> It's kept my nerve focus of subject knowledge up to date and provided content to refer students also about that area, I've got a bit more to say.
>
> **Club Leader**

Some leaders felt that being involved helped them build on good levels of prior knowledge, and that it had provided them with a better understanding of the cyber sector, and that it had provided them with a better understanding of the cyber sector.

Some leaders felt that being involved helped them build on good levels of prior knowledge, and that it had provided them with a better understanding of the cyber sector, and that it had provided them with a better understanding of the cyber sector.

knowledge. One Club Leader taught the National Progression Award (NPA) in Cyber Security and noted that their involvement in CyberFirst and Cyber Discovery had given them a better understanding of the language used on the course. Several said they would value the opportunity to undertake further training and share ideas with other leaders, for example through an online forum or club.

Club Leaders also identified outcomes for the wider school, for example by showcasing to parents that their students are able to access competitions and have the opportunity to progress.

> “Parents are always keen to find out about extra-curricular activities that do not cost anything, but will help stretch their children.”
>
> **Club Leader**

One Club Leader said that where they had particular success with some of their students taking part, they were able to cite that in applications to become a national computing centre.

> “There is kudos attached if you have success. We've also featured students in press releases where they've gone quite a way. It's positive publicity.”
>
> **Club Leader**

As mentioned above in the ‘reasons for taking part’ section, Club Leaders in CyberFirst accredited schools are able to use Cyber Discovery to help achieve their wider aim to encourage students to engage with computer science and the application of cyber security in everyday technology.

Programme impact and the skills gap

This section assesses the potential contribution of Cyber Discovery to closing the cyber skills gap. This is a long-term programme aim and there are many factors that may help close the gap. Measuring the precise impact of Cyber Discovery on the skills gap is beyond the scope of the evaluation as this would likely include the development of a counterfactual approach to assess whether any participant outcomes would have occurred regardless. As a result, brief information is included to cover initial perceptions around whether the programme may be closing the gap and suggestions from qualitative interviews as to how this could be maximised.

Perceptions of the skills gap and existing mechanisms

As noted in the Introduction, it is estimated that 48% of businesses in the UK have a basic technical skills gap in areas including setting up configured firewalls, storing or transferring personal data, and detecting and removing malware. Research has also shown that there are misconceptions about the skills required to fulfil a cyber security role and highlighted the need for candidates with a broad set of technical expertise and skills, complemented by the right soft skills to do the job effectively.

Students generally felt that the programme would help to close the gap, albeit that this largely reflected their own positive experiences of the programme. Most felt that they would probably have had an interest in cyber security, but without taking part they would not have had the same level of insight into the sector. This helped some to refine their future career plans with, as seen earlier, data showing that the proportion of respondents very interested in a cyber security career did not increase from pre to post stages.

In Years Two and Three of the evaluation, industry experts shared their views on the skills gap and suggestions for further action. As discussed, experts highlighted a range of benefits which they felt was evidence of the potential of the programme to contribute to closing the skills gap. For example, some had recruited placement students and apprentices and noted that participants, particularly those reaching Elite stage, tended to be high calibre candidates.

Cyber Discovery was felt by some experts to address the key area of the skills pipeline by encouraging a diverse range of students to pursue a cyber security career who otherwise may have entered technical roles in other sectors. As many students are still in education, it was recognised that it may be years before the impact is realised. However, experts were confident that Cyber Discovery was raising awareness of roles in the sector and equipping students with the knowledge and skills needed.

> “Cyber Discovery has broadened my knowledge of the roles that the umbrella term of cyber-security covers, and it's not all hacking. There's the forensics and reverse engineering malware side, which I have almost fallen in love with. And this was all due to Cyber Discovery, which led me to google and expand my horizons.”
>
> **Year Four student**

One student noted that it was particularly beneficial to take part in a government led programme rather than one that was industry sponsored. They saw a greater role for an organisation such as the National Cyber Security Centre (NCSC) in communicating the pathways into the sector. “SANS will channel you to GIAC, OffSec will channel you somewhere else. It would be nice if the NCSC played a greater role in communicating with young people.” Year Four student

Additional mechanisms to close the skills gap

A range of views were presented on the priority areas to reduce the skills gap, with common themes being a lack of specialist knowledge and the lack of alignment between the demands of industry and what potential candidates are taught in formal education. Some felt that graduates often had a clear grasp of theoretical issues but struggled to apply their knowledge to a business setting. In their view, educational establishments should be supported to give better industry specific careers guidance to students, for example how to answer behavioural questions and complete psychometric tests.

Regional differences were highlighted, for example the problem of ‘brain drain’ where graduates in certain areas leave because they do not think high value industry and progression are available to them there.

Another felt there was a gap in certain specialisms. In their experience, candidates tended to have a general technology focus rather than having a specialism and were often not aware of the range of roles available to them, especially with ethnic minority groups and female candidates. They suggested that any initiative should be representative of the whole sector and feature a diverse range of roles, for example less emphasis on pen testers. It was suggested initiatives do more to recognise the breadth of the portfolio, for example making sure that training is aligned to the wider elements of cyber security, including compliance, governance, risk and strategy.

A further theme was the need to improve public knowledge of cyber security. It was noted that parents, teachers and friends were all likely to influence students' decisions about careers, therefore requiring wider acceptance of cyber security as a viable careers option. This is supported by survey data, which showed that for around a quarter of respondents, their decision to participate in Cyber Discovery was influenced by a teacher or friends. Another industry expert identified a gap in further and higher education:

> “When you get to sixth form or college, it's all gone.”
>
> **Industry expert**

They suggested that there is a need for a continuous pathway to ensure that when young people are focused on apprenticeship or job applications, they retain their focus and interest in cyber security. They proposed an expansion of the University Technical College (UTC) model, with business sponsored projects based around industry problems. This links to qualitative feedback from curriculum experts and Club Leaders who would like to see formal cyber security qualifications introduced, for example a GCSE or T-Level. As noted in the ‘links to the curriculum’ section, it was suggested that this could provide an alternative to the “programming-heavy” computer science courses, which can put off female students.

> “We're definitely crying out for a vocational GCSE as an alternative to computer science. There's a real market for a GCSE in cyber security, especially for girls. They love that problem solving element, the idea of doing good in the world is really motivating. Programming less so.”
>
> **Curriculum expert**

Students suggested that programmes could give them more information about the specific requirements for entry level roles in the sector and where to find jobs.

> “The whole industry doesn't seem very accessible. There aren't too many jobs around and it's not clear what you need for each job. There are no subjects in school for it. There certainly isn't a shortage of people who want to get into it, but some decide they want to be a software developer instead because it's more clear what you need to learn.”
>
> **Year Four student**

Conclusions and recommendations

This section provides a short conclusion drawing together the main strands of evidence followed by a core set of recommendations.

Conclusions

The programme met the key performance indicator in the original contract. This was to engage almost 6,000 participants by the end of the fourth year, with the overall number of those registering increasing from 27,903 in Year Two to 35,941 in Year Three, dropping to 28,232 in Year Four.[footnote 29]

In the final two years, the programme exceeded the soft target of 30% females introduced at Year Three. This was achieved in part through opening up the programme to 13-year-olds and targeting females in this age range. Participation appeared highest in areas with lower levels of deprivation and, in England, outside the South. The large difference in engagement across regions suggests the potential for wider geographic growth, but also highlights difficulties in achieving regional diversity. The proportion of ethnic minority participants was higher for Cyber Discovery than for computer science GCSE or A Level equivalents.

Participants generally progressed positively through the programme. Some struggled in the initial stages, potentially as despite a relatively gradual introduction there may always be some students that are not suited to the programme at that time. The programme provided additional training to 590 most talented participants through Elite Camps, and there was a high pass rate among those who went on to sit GIAC exams. Participants felt there was enough support in place, and one theme from Club Leader interviews was feeling that they could be helped more to support students in their clubs.

Over a third of Cyber Discovery participants (38%) had taken part in other programmes recently and many were also interested in a wide range of careers and subjects. They were very interested in cyber security but were by no means solely focused on this for future subject choices or careers. They took part in the programme largely to improve their skills, although a large minority did see the programme as helping them with possible careers.

Participants enjoyed taking part in the programme, finding it engaging, positive and useful. They felt it was challenging – although some struggled in the initial stages, they generally saw the level of challenge, often going far beyond the cyber security content of the Computer Science GCSE, as a strength of the programme. They felt tested and enjoyed proving their ability. Evidence suggests that this linked to the main strength of the programme in directly improving cyber security skills.

Survey data shows self-reported participant improvements in relevant cyber security skills, and their understanding and knowledge of job requirements but there is no evidence that this translates into increased interest in studying cyber or taking up a relevant career.

The lack of evidence of increased interest may be due to the small sample size, that providing relevant information made some realise it was not a relevant career for them earlier than they might have, or that external factors unconnected with the programme had a negative effect. It may also be the case that for many students, interest in cyber security careers was already high before participating in Cyber Discovery, so interest levels remained similar rather than increasing. Interviews suggested that for some students, the programme confirmed their interest in the subject rather than introducing a new idea. Those attending Elite Camp felt they benefited from the careers advice provided during this phase, with there being less evidence that those who did not reach this stage directly picked up career information. The relative lack of cyber career information in the early programme stages may also explain the lack of evidence of positive change in cyber career interest. Furthermore, lack of evidence around change in cyber career interest may reflect the fact that the initial objective of Cyber Discovery was to identify and support an elite cohort of already engaged and talented individuals, rather than to target a wider audience.

Industry experts were very positive about their involvement, again feeling that the Elite phase was particularly beneficial. They felt that Cyber Discovery helped develop the skills of the most talented attending the Camp and were positive about the range of different students attending.

Recommendations

While the main body of the report provides many specific recommendations, the following broad underpinning areas are included below. The first set of recommendations relate to the programme itself while the second set of recommendations relate to the positioning of Cyber Discovery in the wider marketplace, largely drawing on suggestions from curriculum experts and industry experts about what more could be done to address the cyber security skills gap.

Programme recommendations

Programme Recommendation 1: Continue to increase diversity

Increasing the diversity of those taking part in Cyber Discovery is important not only in its own right but also for ethical reasons and as a potential means to reduce the skills gap. This reflects well-known challenges in the sector and across STEM subjects as a whole in this area. This is also important given that around a third of participants did not agree strongly or agree that cyber security careers were open to everyone regardless of background.

Data in this report suggests that opening the programme to those aged 13 has made a considerable contribution to increasing gender diversity across the programme, in part likely due to targeted marketing to girls in this age group. This cohort should be tracked in detail to begin to assess whether their participation at this stage facilitates engagement beyond what was achieved in previous years where the programme was only open to those aged 14 and over.

Further programme and sectoral learning can build on information in this report on successful approaches for engaging female students. It is important that these key strengths are built upon, for example facilitating communities of female students. Similar approaches should be examined for socio-economic diversity, examining issues identified in this report on access to suitable technology, raising awareness of bursaries and apprenticeship routes to remove perceived financial barriers to higher education, and the overall reach to schools in deprived areas. This may be particularly important given the relatively high level of interest in studying or having a career in cyber security among those in state schools compared to those in private or other types of school.

Programme Recommendation 2: Examine and embed career consideration

As the Theory of Change details, a key intended impact of Cyber Discovery is that it helps improve consideration and take-up of cyber security careers, thereby contributing to reducing the cyber security skills gap. Therefore, the extent to which Cyber Discovery changes career consideration is a crucial question for future programme development. Information in this report suggests it should not be automatically assumed that taking part leads to improved career consideration although it may be that increased knowledge leads to a better alignment of career options among participants, including some understanding it is less of an option for them.

Further work is required to provide a solid evidence base on this issue. This could include embedding simple questions on career consideration into any registration (at least for those aged 16 and over who can provide consent), with this facilitating longer-term follow-up and potential links to later administrative data on further and higher education choices.

Information on careers throughout the programme should be expanded to ensure that this is not just prioritised at Elite Camp stage. This should include making information as transparent as possible to Club Leaders given the lack of confidence and availability of resources affecting some.

Programme Recommendation 3: Improve support and guidance for Club Leaders and students

Improved support and guidance should be provided to Club Leaders to enable them to better engage students and assist them through the challenges. Firstly, there is a need to ensure that approaches to engagement taken by Club Leaders are best suited to their specific needs. It is appropriate for Club Leaders to take a broad approach to engaging young people, particularly as this may help both create and sustain an interest in cyber security and ensure the programme continues to avoid focusing on computer science students. The challenge is to ensure that leaders and students have expectations set at realistic levels to avoid being put off participation or careers if they do not progress as planned.

The second area is ensuring that participants and Club Leaders have adequate support and guidance available on Cyber Discovery itself. Evidence from interviews suggested that some Club Leaders struggled to provide consistent support and guidance with challenges. A range of possible approaches to supporting leaders are provided in the “support and guidance for participants” section, including video walkthroughs, more signposting resources, and an online community for them to share ideas and experiences.

Wider recommendations

Wider Recommendation 1: Consider the role of formal qualifications

A strong theme from interviews with Club Leaders and students was that the content of Cyber Discovery goes far beyond what is covered in relevant computing courses, including GCSE and A-Level Computer Science. Rather than incorporating more curriculum content into Cyber Discovery or vice versa, some curriculum experts and Club Leaders suggested that they would like to see the introduction of formal cyber security qualifications, such as a GCSE or T-Level in Cyber Security. In their view, this could present an alternative to computer science qualifications, which some students (particularly female students) find too programming heavy and this can deter them from the subject. This has important implications for addressing diversity in cyber security.

Some students found the extra-curricular aspect of Cyber Discovery highly appealing and felt that a programme that tied closely to what they were studying in school may not be as engaging and fun. Feedback also suggested that the opportunity for independent learning and research was an important outcome.

Wider Recommendation 2: Consider non-technical cyber security roles

Students generally felt that Cyber Discovery provided them with an improved understanding of the cyber security sector and the diversity of roles available. However, it was suggested that careers information was targeted towards technical roles, such as ethical hacking and digital forensics. Students and industry experts proposed that future programmes could include content relating to a wider range of cyber security roles, such as governance, policy, strategy and risk.

Wider Recommendation 3: Consider the scope of the overall cyber security portfolio

This evaluation highlights the extent that those taking part in Cyber Discovery not only have participated in other computing or cyber security programmes but that around two-thirds (65%) were considering doing so in the future. Data suggests that those taking part in the evaluation have enjoyed Cyber Discovery and feel they have benefitted. Qualitative feedback suggested that some preferred Cyber Discovery to other programmes, although there were suggestions that other programmes had certain strengths as well.

Survey data suggests that Cyber Discovery may have a distinct image compared to other programmes, in particular being seen as more challenging and providing a longer time frame so students can take part in their own time around other commitments. Cyber Discovery also provides a high-level of achievement for the most talented, including very high levels of certification via the GIAC exams in the Elite phase.

The image and offering of Cyber Discovery needs to be considered in line with the rest of the CyberFirst portfolio and other existing or potential programmes. While developing the skills of the most talented, Cyber Discovery also engages large numbers of participants, many of whom develop skills and progress through the programme but without reaching Elite Camp stage. Developing the offering into a year-round learning option would provide opportunities to engage more students on a regular basis.

This represents an ongoing challenge across the CyberFirst portfolio as a whole, in understanding the contribution of different interventions in terms of:

- engaging a broad base of participants, particularly in the early years when curriculum options are still open
- identifying the most talented and ensuring there is sufficient support in place to facilitate career choice, especially among older participants
- ensuring that a sensible balance is in place across any portfolio, with similar options being potentially valuable but only if this provides genuine choice, is not confusing to participants or schools, and enables cross-programme sharing of learning

Appendix One: Theories of Change

2018 Theory of Change:

2020 Theory of Change:

Appendix Two: Tables and Figures

Table 9: Demographics for participants registered for Assess by year

	Year One	Year Two	Year Three	Year Four
Gender[footnote 30]				
Female	21%	25%	32%	33%
Male	79%	75%	68%	67%
Age[footnote 31]				
13	NA	NA	28%	27%
14	36%	36%	26%	24%
15	29%	23%	19%	18%
16	20%	17%	14%	16%
17	12%	20%	11%	11%
18	4%	3%	3%	5%
Country[footnote 32]				
England	100%	93%	88%	88%
Northern Ireland	NA	1%	2%	1%
Scotland	NA	5%	7%	8%
Wales	NA	1%	3%	3%
Status[footnote 33]				
Club participants	56%	51%	53%	41%
Non-club (individuals)	44%	49%	47%	59%
Whether new or returning [*34]				
New	NA	84%	82%	74%
Returning	NA	16%	18%	26%

Source: Management information.

1. National Security Strategy and Strategic Defence and Security Review 2015 ↩
2. Cyber security skills in the UK labour market, 2021 ↩
3. Initial National Cyber Security Skills Strategy ↩
4. Joint Committee on the National Security Strategy ↩
5. CyberFirst is delivered by NCSC and aims to develop “the UK's next generation of cyber professionals through our student bursaries, courses for 11-17 year- olds and competitions”. This includes Cyber Discovery, Cyber First Girls Challenge and the Cyber Schools Hub. Further details can be found at the CyberFirst Girls Competition webpage. ↩
6. Cyber Schools Programme Guidance ↩
7. Search to find Cyber Security experts of the future, press release ↩
8. Initial National Cyber Security Skills Strategy: increasing the UK's cyber security capability - a call for views, Executive Summary ↩
9. In Year One, ‘elite students’ were defined as students scoring 13 or 14 on CyberStart Assess (out of a maximum possible score of 14), having broken into HQ level 10 and 11 (completing at least one challenge. ↩
10. SANS management information; “Cyber Discovery Year Two: Close of Game and Essentials Report”, p12 ↩
11. This is supported by analysis of self-reported interest in cyber security on a scale of one to ten: the mean for Year Three pre-survey was 7.8, compared to 9.4 for Year Four single point survey. ↩
12. This includes some participants registering in multiple years. ↩
13. Unlike in previous years, there was no pre-registration campaign in Year Four due to it opening earlier in the year. As a result, everyone who registered in Year Four gained instant access to Assess. ↩
14. Game registrations as a percentage of all registrations dropped between Year One and Year Two as the qualification bar was raised. ↩
15. In Year One, ‘elite students’ were defined as students scoring 13 or 14 on CyberStart Assess (out of a maximum possible score of 14), having broken into HQ level 10 and 11 (completing at least one challenge in both) and having “demonstrated keen interest in the cyber security industry” (Cyber Discovery Year 2 Close Of CyberStart Assess Report). ↩
16. There was no Elite Camp in Year Four. ↩
17. The Roehampton Annual Computing Education Report: Data from 2017 ↩
18. LG Inform, IMD IDACI score England ↩
19. This is used as a proxy measure due to the different age groups: Cyber Discovery being open to young people from 13-18, while IDACI provides data for those aged 0-15. ↩
20. For Year Three, details were provided for 3,393 schools, of which 2,891 were in England and 2,878 were successfully matched to IDACI deciles. For Year Four, details were provided for 3,011 schools, of which 2,621 were in England and 2,615 were successfully matched. ↩
21. Population estimates for the UK, England and Wales, Scotland and Northern Ireland: mid-2019 ↩
22. The Roehampton Annual Computing Education Report: Pre-release snapshot from 2018 ↩
23. https://cyberdiscoverycommunity.uk/ ↩
24. Change is calculated prior to rounding pre and post figures, so does not always correspond exactly to change observed between rounded figures. ↩
25. This question uses identical statement wording in relation to science used in the 2019 Science Education Tracker Wave 2, Young People's Views on Science Education. Questions were asked of a nationally representative sample of Year 7 to 13 students in England about science. ↩
26. DCMS (2020) Cyber security skills in the UK labour market ↩
27. Since some participants participated in Cyber Discovery across more than one year, it is possible that the same participant may have been identified as Elite in more than one year. ↩
28. The Roehampton Annual Computing Education Report: Data from 2017 ↩
29. A discussion about the possible reasons for a decline in the number of registrations in Year Four is presented in the ‘Total participation’ section above, centred around the impact of school closures. ↩
30. Percentages for gender are calculated on base sizes of 17,264, 24,296, 35,887, and 28,232 for Years One to Four respectively. These bases do not include very small proportions of participants who reported another gender or did not state their gender. ↩
31. Age percentages for Years One and Two are not directly comparable with Years Three and Four, where the minimum age was lowered to 13. Percentages for age are calculated on base sizes of 16,845, 24,742, 33,536, and 28,253 for Years One to Four respectively. ↩
32. In Year One the programme was only available in England. Percentages for country are calculated on base sizes of 23,692, 34,120, and 28,232 for Years Two to Four respectively. ↩
33. Percentages for club and non-club participants are calculated on base sizes of 18,293, 24,251, 35,570, and 28,232 for Years One to Four respectively. ↩

Is this page useful? Yes No Report a problem with this page

Coronavirus (COVID-19)

Coronavirus (COVID-19): guidance and support

Brexit

Check what you need to do

OGL All content is available under the Open Government Licence v3.0, except where otherwise stated

© Crown copyright