KPMG

A study into the effectiveness of CyberEPQ

A KPMG report for the Department for Science, Innovation and Technology

May 2025

Important notice

This report ("Report") has been prepared by KPMG LLP ("KPMG") solely for the Department for Science, Innovation and Technology ("DSIT" or the "Client") in accordance with the terms of engagement contract agreed between DSIT and KPMG, dated 3 January 2025 ("Contract"). The Client commissioned the work to assist in its consideration of the effectiveness of the CyberEPQ. The agreed scope of work is included in Section 1 of this Report.

The Client should note that our findings do not constitute recommendations as to whether or not the Client should proceed with any particular course of action.

This Report is for the benefit of the Client only and it has not been designed to be of benefit to any other party. In preparing this Report we have not taken into account the interests, needs or circumstances of anyone apart from the Client, even though we may have been aware that others might read this Report.

This Report is not suitable to be relied on by any party wishing to acquire rights against KPMG (other than the Client) for any purpose or in any context. Any party other than the Client that obtains access to this Report or a copy (under the Freedom of Information Act 2000, the Freedom of Information (Scotland) Act 2002, through the Client's Publication Scheme or otherwise) and chooses to rely on this Report (or any part of it) does so at its own risk. To the fullest extent permitted by law, KPMG LLP does not assume any responsibility or liability in respect of this Report to any party other than the Client.

In particular, and without limiting the general statement above, since we have prepared this Report for the benefit of the Client alone, this Report has not been prepared for the benefit of any other Government Department nor for any other person or organisation who might have an interest in the matters discussed in this Report.

We have not verified the reliability or accuracy of any information obtained in the course of our work, other than in the limited circumstances set out in the Contract.

Our work commenced on 3 January 2025 and our fieldwork was completed on 10 March 2025. We have not undertaken to update our Report for events or circumstances arising after that date.

This engagement is not an assurance engagement conducted in accordance with any generally accepted assurance standards and consequently no assurance opinion is expressed. Nothing in this Report constitutes a valuation, tax or legal advice.

Contents

Executive Summary

Overview of the study

DSIT plays a key role in delivering the Government's digital and cyber-related commitments, including in helping to address skills shortages in the cyber security labour market. One of the ways DSIT aims to do this is through the Cyber Extended Project Qualification (EPQ), which is a Level 3 qualification in cyber security open to people aged over 14 years old. The CyberEPQ aims to develop young people's cyber security skills and inspire them to pursue a career or further education in cyber security. It is delivered by the Chartered Institute for Information Security (CIISec) via an online learning platform (the 'Moodle'), with teachers in the schools/ colleges providing the CyberEPQ often also acting as supervisors for the students' learning. DSIT provided grant funding to CIISec in the financial year (FY) 2023/24 to support student access to the learning and qualification.

DSIT commissioned KPMG to undertake independent research into the effectiveness of the CyberEPQ, focussing on the grant funded places only. The study seeks to answer a limited number of research questions (set out in section 1.2), through a mixed methods qualitative and quantitative approach. This included analysis and triangulation of evidence from documentation, and primary and secondary data, including a combination of surveys, interviews and focus groups with grant funded students, teachers supporting the delivery of the CyberEPQ in their schools/ colleges, and with the delivery partner CIISec. The findings of the study are set out in this report and summarised below.

Key study findings

Effectiveness in building young people's interest and skills in cyber security

The CyberEPQ aims to develop students' knowledge and skills, and in turn build students' interest in studying computing or cyber security further, and in the longer-term pursuing cyber security related careers. In order for the CyberEPQ to do this, students need to enrol on the course and the course needs to be delivered effectively.

Enrolment and course delivery: For the CyberEPQ to build young people's interest and skills in cyber security it is necessary for students to enrol on the course and for the course to be delivered effectively. The target for CIISec for FY 2023/24[1] was to enrol 400 students[2] through funded places, however, this target was not met. In total 279 students enrolled. The main reasons provided by CIISec as to why this target was not met, included the grant funding being received late, and the impact the COVID-19 pandemic was still having on schools.

Knowledge and skills: Despite not meeting the target number of enrolments, the students who did take the CyberEPQ reported a range of benefits. These included improved knowledge and skills related to cyber security, and also broader, transferable skills. The most frequently reported benefits by respondents to the student survey were improved research skills reported by 13 out of 16 student respondents (81%), and improved knowledge of the topics covered reported by 12 student respondents (75%). Across all topic areas covered by the CyberEPQ, over half of student survey respondents said that their knowledge/ skills had improved to a moderate or great extent.

Interest in studying cyber security: The findings suggest that the CyberEPQ has helped to develop some students' interest in studying cyber security. 6 out of 15 student survey respondents (40%) said that taking the CyberEPQ had increased the likelihood of them studying cyber security at university (either to a small, moderate or great extent), and 4 out of 15 student respondents (27%) said that it had increased the likelihood of them studying computing at university. However, a proportion of students reported CyberEPQ had no impact; 7% said it had no impact on their plan to study cyber security at university as this was always what they were intending to do, and 27% said it had no

---

[1] Elsewhere in the report all years refer to academic years rather than financial years, unless stated otherwise.
[2] CIISec CyberEPQ: 2023-2024 Overview of Activities, Summary & Reflection

impact on their plan to study computing at university as this was always what they were intending to do.

While it was acknowledged that, in general, students taking the CyberEPQ were those with a prior interest in the subject, different reasons were offered by teachers and CIISec as to how CyberEPQ has helped develop students' interest in studying cyber related subjects further:

— One teacher in the focus group said that CyberEPQ enabled students to test whether they enjoyed cyber security so that they could be more certain about deciding to pursue further study or a cyber security career.

— CIISec thought that students sometimes surprise themselves with what they are interested in and therefore may consider studying cyber security as a result of taking the CyberEPQ which they may not have otherwise done.

Interest in pursuing cyber security careers: A longer-term intended impact of the funded places for the CyberEPQ is to increase the number of students going on to pursue cyber security careers. As well as making students more aware of jobs in the sector, talks delivered by alumni students also aim to raise awareness of employment opportunities.

The evidence shows that 6 out of 16 student respondents (38%) said that taking the CyberEPQ had given them a better understanding of career opportunities in the cyber sector and for some students, although not all, the CyberEPQ had influenced their future career plans. While 4 out of 15 students (27%) responded that it was not their future plan to seek a career in cyber security or computing, 9 out of 15 student respondents (60%) said that taking the CyberEPQ had increased the likelihood of them seeking a career in cyber security (either to a small, moderate or great extent), and 8 out of 15 student respondents (53%) said that it had increased the likelihood of them seeking a career in computing. Some teachers participating in the focus groups considered that the students taking the CyberEPQ were those that already had an interest in cyber security careers. Therefore, they considered it was difficult to determine if it was the CyberEPQ that had helped develop students' interest in cyber security careers.

Effectiveness in meeting the grant objectives

The three agreed objectives for the funding from DSIT to support the delivery of the CyberEPQ were:

— to enrol students from diverse and geographically spread backgrounds;

— to build industry partnerships and match funding to make the CyberEPQ more financially sustainable; and

— to update the content on the online learning platform.

Achieving diversity in enrolments: The monitoring data indicates that the students taking funded places for the CyberEPQ are not fully representative of the UK student population. For example, around 25% of students were females, and the places were also not geographically spread across the UK, for example, 23% of students were from the West of England while no students were from Tees Valley. The predominant ethnic group of students was White British (63%) (compared to 82% in the UK population).[3]

CIISec stated that they try to achieve diversity in enrolments in a variety of ways such as by making clear to teachers that the CyberEPQ should be made available to everyone, not just students taking computing, having specific materials for girls to advertise the CyberEPQ course, and trying to keep students in year 9 who take the Headstart[4] course engaged through practical cyber security-related activities. Teachers in the focus groups also noted the challenges, particularly in terms of increasing the number and proportion of female students taking the CyberEPQ. One teacher said that this was part of the wider issue of encouraging females to study STEM (Science, Technology, Engineering and Maths) subjects. Females made-up 42.8% of A level entrants in core STEM subjects in 2024.[5] The

---

[3] This is used as a proxy for the ethnicity of students for the purposes of comparison with students taking the CyberEPQ.
[4] Headstart - CIISec
[5] A Level Results 2024 - WISE The proportion of female entrants varies across subjects. The proportion of female entrants was 17.5% for computing, 63.5% for biology, 56.2% for chemistry, 23.3% for physics and 37.2% for maths.

percentage of girls studying the CyberEPQ being substantially less than this (at 25%) suggests more could be done to encourage take-up among females. As detailed in section 3.3, a number of ideas were suggested that could help encourage participation among female students.

Building industry partnerships and developing match funding: There was no specific target set in relation to this grant objective, and there was no data available/ provided on the number of industry partners developed in 2023/24 or the amount of matched funding obtained to assess performance against this grant objective. CIISec said that they had not delivered on the grant objective "to build industry partnerships and match funding to make the CyberEPQ more financially sustainable" in 2023/24. However, CIISec reported that some progress has since been made to raise additional match funding. A key action taken by CIISec is to change the approach to obtaining sponsorship for CyberEPQ students from its corporate members.

Adding new content to the online learning platform: The CyberEPQ is delivered via an online learning platform. While it is a grant objective to add new content, no targets are set in terms of the volume of content or in relation to what it should cover. In September 2024 new content was introduced on the online learning platform to cover two new topic areas: AI and quantum. Some teachers in the focus group said that the new modules were particularly good and had received positive feedback from students.

Unintended consequences of the CyberEPQ

Neither CIISec nor teachers generally thought there had been any unintended consequences – either positive or negative – of the CyberEPQ. CIISec said that because the CyberEPQ has been delivered in a similar way since 2016, there is less likelihood of unintended consequences arising now.

1 Introduction

1.1 Context for the study: About CyberEPQ

As set out in the AI Opportunities Action Plan,[6] government's vision is for the UK to be a leader in AI. It is recognised that cyber security is fundamental to achieving this ambition and is critical to the UK's economic resilience.[7]

However, there is a skills shortage in the cyber security sector which needs to be addressed in order to achieve this ambition. The Cyber Security Labour Market Survey 2024 shows an annual shortfall of approximately 3,500 people needed to join the workforce in 2023.[8] It also found that, in the UK:

— 44% (637,000) of businesses have skills gaps in basic technical cyber areas;[9] and
— 27% (390,000) of businesses have gaps in advanced skills, such as penetration testing.

From a diversity perspective, the survey found that:

— 15% of the cyber security workforce are from ethnic minority backgrounds; and
— 17% of the cyber security workforce are female.

DSIT plays a key role in delivering the Government's digital and cyber-related commitments, including in helping to address the skills shortage. DSIT and the National Cyber Security Centre (NCSC) deliver several cyber skills initiatives targeting the under 25s which aim to engage young people in cyber in order to improve cyber security skills and encourage entry into the cyber security workforce. This includes: the CyberFirst Girl's competition for 12 to 14 year olds; Cyber Explorers, which is an online learning platform for 11 to 14 year olds; and the Cyber Extended Project Qualification (CyberEPQ), which is a qualification for 16 to 18 year olds.

The CyberEPQ, which is the focus of this study, aims to develop young people's cyber security skills and inspire them to pursue a career or further education in cyber security. It is an enhanced version of the Level 3 EPQ, a qualification normally taken by students alongside A levels, and is accredited by City & Guilds. The CyberEPQ was first introduced in 2016/17 and is the UK's only EPQ in cyber security and was developed by a consortium of education and cyber security partners. It is delivered by the Chartered Institute for Information Security (CIISec), with DSIT providing grant funding to CIISec in the financial year (FY) 2023/24 to support student access to the learning and qualification.

Key features of the CyberEPQ include:

— The course content includes compulsory modules and specialist modules, covering topics from computing history to incident response management.
— It utilises a distance learning platform (the 'Moodle') to enhance geographic reach.
— There are no formal entry requirements (aside from students being over 14 years old), in order to try to widen access and improve diversity.

173 students participated in the CyberEPQ in the academic year 2023/24[10], from a range of state, independent and sixth form colleges, as well as independent students, of which 121 were grant funded students.[11]

---

[6] AI Opportunities Action Plan - GOV.UK
[7] Cyber security sectoral analysis 2025 - GOV.UK
[8] Cyber security skills in the UK labour market 2024 - GOV.UK
[9] These cover the technical areas covered under the Cyber Essentials scheme.
[10] Unless otherwise stated all years refer to academic years rather than financial years in the report.
[11] CIISec CyberEPQ: 2023-2024 Overview of Activities, Summary & Reflection.

1.2   About the study

As Government has a responsibility to maximise public value and the outcomes delivered for taxpayers' money, DSIT has commissioned KPMG to undertake independent research into the effectiveness of the CyberEPQ. The scope of this study is limited to the granted funded part of the CyberEPQ in 2023/24.

The study seeks to answer the following research questions which were agreed with DSIT at the outset:

1   To what extent are CyberEPQs effective in building young people's interest and skills in cyber security?

2   How effective has the delivery partner been in meeting the grant objectives, particularly around:
— Diversity in enrolments;
— New content in the online learning platform; and
— Building industry partnerships and developing match funding?

3   What, if any, unintended consequences of the CyberEPQ have there been?

The purpose of this study is to provide evidence to inform DSIT's case-making for future grant funding, inform continuous improvement of delivery of the CyberEPQ and enable DSIT to understand and report on the effectiveness of the CyberEPQ. This is narrower in scope than a formal evaluation given the resource and budget available. In particular, although this study includes elements of process and impact evaluation, it does not include a value for money assessment, and there is no counterfactual to allow for a robust assessment of the impact of CyberEPQ and the attribution of impacts to the CyberEPQ. This study focuses on answering the evaluation questions above.

1.3   The approach to the study

In this study a range of approaches were used to gather evidence in order to answer the research questions. The study was designed to align with good practice guidance including the HM Treasury Magenta[12] and Green Books,[13] Government Social Research Professional Guidance[14] and Government Analysis Function guidance.[15]

The research questions were answered through a mixed qualitative and quantitative approach, which included analysis and triangulation of evidence from documentation, and the primary and secondary data.

To understand how the CyberEPQ is expected to achieve its objectives, a theory of change was developed. The theory of change identifies the associated outcomes and impacts, from the inputs and activities involved in the delivery of the CyberEPQ. The theory of change was developed based on a review of background documents on the programme as well as input from DSIT. Section 2 presents the theory of change and describes the pathways through which expected impacts arise.

To gather the evidence required to answer the research questions, primary research was conducted. The primary research involved:

— A quantitative survey with grant funded students. 140 emails inviting students to participate in the survey were sent[16] (to students completing the 1 or 2 year CyberEPQ course) from CIISec, and 20 survey responses were received. The survey was open from 13th February to 10th March. Of the 20 survey responses, 17 respondents had completed the CyberEPQ and 3 were still studying for the qualification.

---

[12] HMT_Magenta_Book.pdf
[13] The Green Book
[14] Government Social Research. 2021. Ethical Assurance for Social and Behavioural Research in Government
[15] Questionnaire design guidance – Government Analysis Function
[16] 5 undelivered notifications were received.

— 30 minute interviews with two grant funded students. The research plan was to conduct a focus group with grant funded students. However, there was an insufficient number of students willing to participate. All students that were asked to complete the quantitative survey were invited to participate in the focus group. 4 students said they were willing to take part but only 2 subsequently responded to emails to organise a time for the discussion.

— A 90 minute focus group with teachers delivering the CyberEPQ. 37 emails inviting teachers to participate in focus groups were sent by CIISec and 10 teachers said they were willing to take part. The arranged date and time of the focus group resulted in 6 teachers participating.

— A 1 hour interview with CIISec.[17]

Bespoke research instruments including surveys and topic guides were designed in line with best practice for each element of the primary research described above. A semi-structured approach was adopted for the interviews and focus groups as this was considered optimal to making sure that all relevant topic areas were covered and that there was consistency and comparability in the topic areas covered across the different stakeholder groups engaged, while also maintaining flexibility to explore the issues mentioned in more detail and probe areas of interest.

In addition to the primary research, secondary data was collated from DSIT and CIISec. Secondary data refers to information and data that has already been collected and processed. Analysis of secondary data offers a cost-effective and efficient way of answering the research questions in this study. The secondary data included:

— A quantitative survey with teachers delivering the CyberEPQ carried out by DSIT in 2024; and

— CIISec CyberEPQ: 2023-2024 Overview of Activities, Summary & Reflection

1.4   Limitations of the study

The following limitations of the study should be considered when reviewing the study findings:

— **Attribution of impacts to CyberEPQ:** This study is narrower in scope than a formal evaluation. Although there are elements of process and impact evaluation, it does not include a value for money assessment, and there is no counterfactual to enable the attribution of impacts to the CyberEPQ.

— **Representativeness of samples:** The limited number of student respondents to the student survey and limited number of student participants in the qualitative research means that the views shared may not be representative of all students. In addition, there is possible self-selection bias across the students and teachers that participated in the research and therefore the views provided may not be representative of the wider population of students taking the CyberEPQ and the teachers offering the CyberEPQ.

1.5   Report structure

The remainder of the report is structured as follows:

— Section 2 sets out the theory of change for CyberEPQ explaining the pathways through which expected impacts may arise. This section includes a logic model which shows visually the causal mechanisms to the impacts and the assumptions upon which it is based.

— Section 3 sets out the findings in relation to each of the research questions. This includes the effectiveness of the CyberEPQ in building young people's interest and skills in cyber security, the effectiveness in meeting the grant objectives and the unintended consequences of the CyberEPQ.

---

[17] A quantitative survey with teachers delivering the CyberEPQ was not carried out as DSIT had conducted one previously and it was therefore deemed disproportionate to undertake a further survey given the time and budget for this study.

2 Theory of Change

2.1 Introduction to the Theory of Change

The theory of change, as illustrated visually in a logic model, demonstrates how the CyberEPQ is expected to deliver its objectives through its inputs and activities, and the outputs, outcomes and impacts associated with this. It forms a key building block for the study that was used to identify the information that needed to be collected in order to answer the research questions.

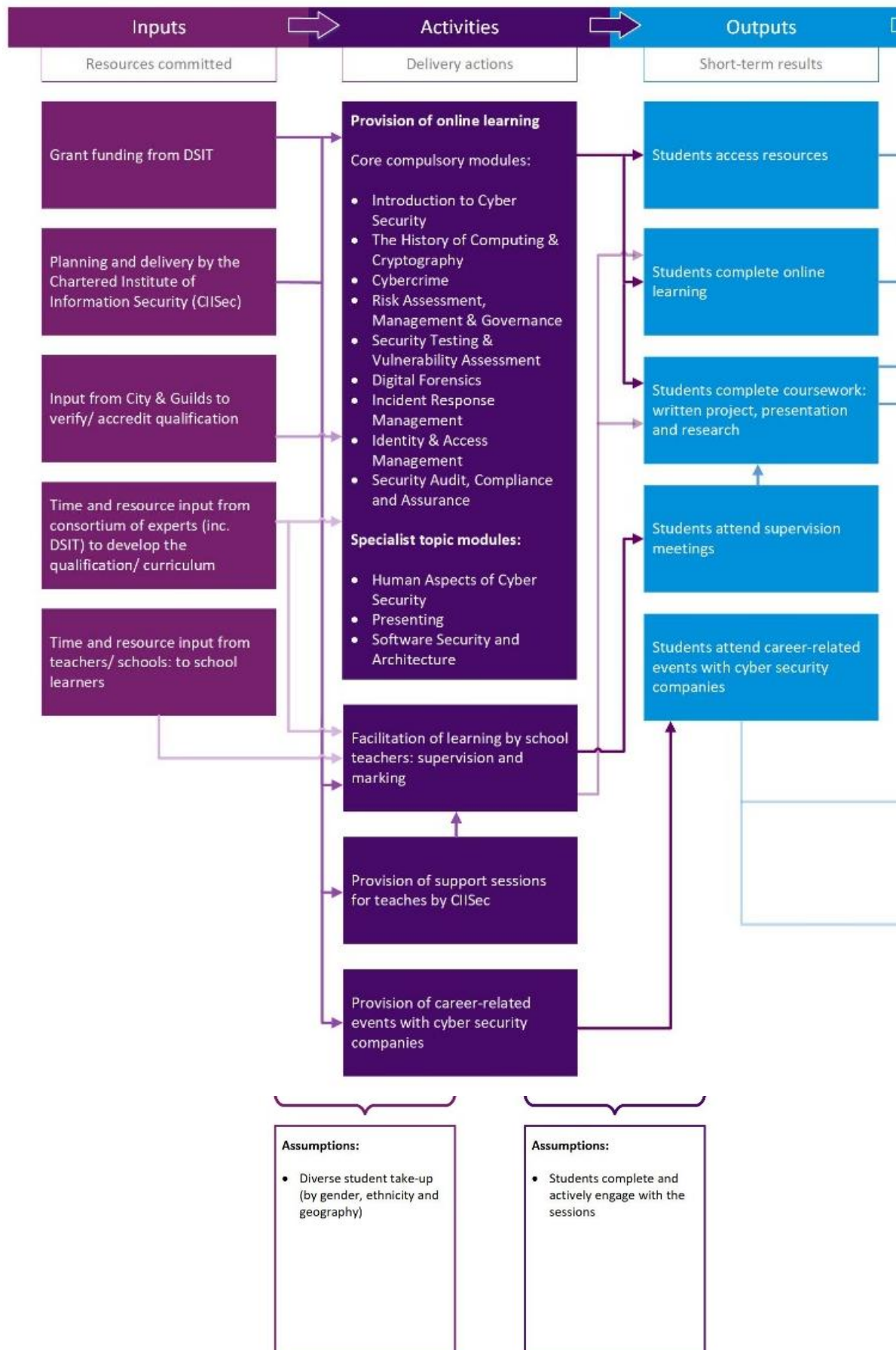The theory of change includes the following elements:

— Inputs: These are the resources committed to the delivery of CyberEPQ.
— Activities: These are the actions taken and the activities provided.
— Outputs: These arise as a result of the various activities delivered.
— Outcomes: These are the expected short- and medium-term effects.
— Impacts: These are the expected long-term effects that arise as a result of the CyberEPQ. The impacts are grouped into intermediate and long-term impacts to reflect the time period over which the impacts are expected to materialise.
— Assumptions: The assumptions are described at each causal step to explain what the intervention is based on.

The theory of change was developed through a review of the background documentation and in consultation with policy officials and analysts at DSIT. It was designed to broadly capture the activities of CyberEPQ. It does not capture bespoke activities that may be provided by some teachers to support some students, or the specific nature of students' research projects.

2.2 Theory of Change for CyberEPQ

The theory of change, illustrated through a logic model, is set out below.

Figure 1: Theory of change for CyberEPQ: split over the following two pages

Inputs	Activities	Outputs
Resources committed	Delivery actions	Short-term results

Inputs:
- Grant funding from DSIT
- Planning and delivery by the Chartered Institute of Information Security (CIISec)
- Input from City & Guilds to verify/ accredit qualification
- Time and resource input from consortium of experts (inc. DSIT) to develop the qualification/ curriculum
- Time and resource input from teachers/ schools: to school learners

Activities:

Provision of online learning

Core compulsory modules:
- Introduction to Cyber Security
- The History of Computing & Cryptography
- Cybercrime
- Risk Assessment, Management & Governance
- Security Testing & Vulnerability Assessment
- Digital Forensics
- Incident Response Management
- Identity & Access Management
- Security Audit, Compliance and Assurance

Specialist topic modules:
- Human Aspects of Cyber Security
- Presenting
- Software Security and Architecture

Facilitation of learning by school teachers: supervision and marking

Provision of support sessions for teaches by CIISec

Provision of career-related events with cyber security companies

Outputs:
- Students access resources
- Students complete online learning
- Students complete coursework: written project, presentation and research
- Students attend supervision meetings
- Students attend career-related events with cyber security companies

Assumptions:
- Diverse student take-up (by gender, ethnicity and geography)

Assumptions:
- Students complete and actively engage with the sessions

KPMG

Outcomes →	Impacts
Medium-term results	Intermediate impacts	Long-term impacts

Outcomes — Medium-term results

- Students have improved cyber security skills and knowledge of topics covered by the course
- Students have improved research, written and presentation skills
- Improved ability for independent learning amongst students
- Students gain qualification/ accreditation
- Students gain additional UCAS points
- Students gain a better understanding of career opportunities in the cyber sector
- Students have increased network/ connections with potential cyber security employers

Impacts — Intermediate impacts

- Increased interest in cyber security-related occupations
- Increased interest in cyber security-related further and higher education/ other courses
- Increased employment opportunities
- Increased cyber hygiene amongst students
- Increased number of students attending university to study cyber security-related course

Impacts — Long-term impacts

- Increased number of individuals take up employment in cyber security-related occupations
- Increase in sector GDP
- Increase in diversity of cyber security sector workforce (by gender, ethnicity and geography)
- Reduction in cyber security sector skills gap
- Improved cyber security for the UK

Assumptions:

- Effective delivery to upskill and share knowledge with students

Assumptions:

- Application and implementation of skills aquired

Key:

- All arrows show the pathways to impacts and different colours/ hues are used to aid readability

The long-term impacts outlined in the theory of change are each described below.

Increased employment in cyber security: It is expected that students will access and undertake the online learning provided and complete the coursework in order to finish the CyberEPQ course and gain the associated qualification. In addition, it is expected that students attend supervision meetings with their teachers and attend the career events provided. This is expected to lead to improved cyber security skills and knowledge of the topics covered by the course among students. Students are also expected to gain a better understanding of the career opportunities in cyber security and develop their network with potential employers. In turn, this is expected to lead to increased interest in cyber security careers and in further study of cyber security, as well as improved future employment prospects for the students in cyber security. Subsequently, this is expected to lead to more people entering the cyber security workforce in the longer term.

Increased diversity of cyber security workforce: The grant funding of students to take the CyberEPQ and the online method of delivery is expected to encourage a diverse student take-up of the course by geography and socioeconomic group. If, in turn, diverse cohorts of students complete the CyberEPQ this is expected to result in a corresponding increase in the diversity of the cyber security workforce, through a similar mechanism to that described above for increased employment in cyber security generally.

Reduction in cyber security sector skills gap: The CyberEPQ was designed by a consortium of education and cyber security partners in order to support students to develop the skills needed for the cyber security sector. It is therefore expected that taking the CyberEPQ leads to improved cyber security skills and knowledge in the relevant areas, as well as improved research, written and presentation skills among the course participants, and improved ability for independent learning. In turn a proportion of students that have taken the CyberEPQ and accumulated the relevant skills and knowledge are expected to enter the cyber security workforce, therefore helping to reduce the sector skills gap.

The expected **increase in the GDP of the cyber security sector** and the expected **improved cyber security for the UK** are related to the impacts described above. If more people enter the cyber security workforce and this supports growth of the sector, the GDP of the sector will increase. In addition, if more people with the relevant skills enter the cyber security sector this is expected to improve cyber security for the UK.

3 Study findings

3.1 Introduction to the study findings

This section sets out the study findings in relation to each of the research questions. This includes the effectiveness of the CyberEPQ in building young people's interest and skills in cyber security, the effectiveness in meeting the grant objectives and any identified unintended consequences of the CyberEPQ.

The findings are based on the analysis of the evidence gathered through the primary research and the secondary data and information provided by DSIT, as set out in section 1.3. When reviewing the findings it is important to consider the limitations set out in section 1.4 relating to the difficulty in attributing impacts to the CyberEPQ and that the views of teachers and students that participated in the research may not be representative of the wider teacher and student populations.

3.2 Effectiveness in building young people's interest and skills in cyber security

One of the key intended outcomes of CyberEPQ is building students' knowledge and skills, and the key intended impacts include building students' interest in studying computing or cyber security further, and their interest in pursuing cyber security related careers. As set out in the logic model, (see section 2) in order for the CyberEPQ to contribute towards delivering these outcomes it is necessary for students to enrol on the course and for the course to be delivered effectively.

In this section, the effectiveness of CyberEPQ in generating these intended outcomes is assessed.

Enrolment and course delivery

The target for CIISec for FY 2023/24[18] was to enrol 400 students[19] through funded places, however, this target was not met. In total 279 students enrolled from across 29 institutions (including 26 schools/ colleges, 2 Police Forces and 1 other organisation),[20] of whom 61 were female.[21]

CIISec provided a number of reasons as to why the target number of students was not met. The main reasons stated included the grant funding being received late, and the impact the COVID-19 pandemic was still having on schools. While not stated in the interview with CIISec, another reason for not reaching this target appears to be that a collaboration with a third-party organisation who wanted to deliver the CyberEPQ to 100 female students in London using their own supervisors didn't come to fruition.[22]

To encourage schools/ colleges to offer the CyberEPQ to students, CIISec explained that they promote the CyberEPQ in a variety of ways, including:

— Emailing schools to explain the course and the benefits

— Sharing promotional materials

— Advertising via social media channels

— Hosting webinars

— Using connections with Computing at School (CAS), STEM Engagement Coordinators, Careers Hubs and Outreach Teams

---

[18] Elsewhere in the report all years refer to academic years rather than financial years, unless stated otherwise.
[19] CIISec CyberEPQ: 2023-2024 Overview of Activities, Summary & Reflection
[20] Information provided by CIISec via email on 13th March 2025.
[21] CIISec CyberEPQ: 2023-2024 Overview of Activities, Summary & Reflection
[22] CIISec CyberEPQ: 2023-2024 Overview of Activities, Summary & Reflection

— Using CyberFirst partnerships

— Speaking at conferences and events

According to information provided by CIISec, the funded places for CyberEPQ were delivered across 26 schools/ colleges in FY2023/24. A number of reasons for providing the CyberEPQ were mentioned by teachers in the focus group conducted, including:

— The growing importance of cyber security across the economy and for the future;

— A personal desire to offer the CyberEPQ and considering it would also be a useful offer to students;

— To provide a second chance for students who may not be able to undertake the general EPQ offered at the school because of it being oversubscribed;

— The opportunity for obtaining UCAS points for students – a reason which was also reported in the teacher survey where 6 out of 16 respondents (38%) cited the "qualification supported university applications" as a reason for providing it;

— To help differentiate students when applying for apprenticeships;

— To improve the offer to students and make the school more competitive in terms of breadth of courses provided among other local educational institutions.

In the teacher survey, the two most frequently cited reasons for providing the CyberEPQ were that it builds interest in cyber security as an option for further study or career (cited by 12 out 16 respondents) and general student interest in cyber security (cited by 9 out 16 respondents).

Teachers in the focus group all said that the CyberEPQ complements their existing computer science curriculum. In particular, they said that the CyberEPQ provides a more in depth understanding for students of cyber security than what is provided by computer science A levels. For one teacher, offering the CyberEPQ was a way for students who had enjoyed studying computer science at GCSE to continue their studies in the area as the school didn't offer computer science A level.

Evidence shows that the approach taken by schools to encourage students to undertake the CyberEPQ varied. Some teachers in the focus group said they targeted students who they considered would be well-suited to the CyberEPQ – because of their interest in relevant subject areas, and as they thought the student could manage the extra workload. Other teachers said they tried to raise awareness of the CyberEPQ among students more generally, either to all eligible students or with computer science and maths students specifically. Some teachers commented that a combination of both these approaches were used. One teacher suggested that more advertisement of what employers think of the CyberEPQ may help to support take-up among students. While it was unclear if teachers found it easy or difficult to encourage take-up among students, one of the difficulties mentioned by teachers in the focus group was persuading senior leadership within the school/ college to offer the CyberEPQ.

The student survey provides some evidence around students' interest in, and motivation to undertake, the CyberEPQ. When students were asked what motivated them to do the CyberEPQ, the most frequently reported reason was because of an interest in cyber security - reported by 9 out of 17 (53%) student survey respondents - followed by gaining an extra qualification/ accreditation - reported by 8 out of 17 (47%) student respondents.

Not all students enrolling on the CyberEQ subsequently complete the course and obtain the qualification. According to data provided by CIISec, 75 students withdrew from the FY 2023/ 24 CyberEPQ cohort. CIISec said this was significantly higher than the usual drop out rate,[23] due to students enrolled through a partnership CIISec formed with one organisation, not being engaged as they hadn't been enrolled through a school.

CIISec reported that the point at which students drop out is often before submission of project proposals and shared that they expected this is because after submitting a project proposal students

---

[23] Although the data has not been made available to confirm this.

will be put under pressure to subsequently submit a project and hence drop out ahead of this point to avoid it.

CIISec considered that students may drop out for a variety of reasons including:

— Having too much work, as students are doing the CyberEPQ alongside A levels, and while for A levels their learning is timetabled, the CyberEPQ has to be done in their own time (while one student interviewed said that they underestimated the time required to complete the research project, almost all (16 out of 18 (89%)) students in the student survey said that they had understood what would be required of them to successfully complete the course with 1 student interviewed mentioning A* examples of research projects provided).

— Students finding the independent learning challenging as they are more used to classroom based learning, with teachers leading their learning (however 12 out of 18 students (67%) in the student survey said they understood how the course would be delivered before starting the course. This was further supported by one of the students interviewed who said that their teacher had explained how the course would be delivered and had shared emails from CIISec about the course delivery).

— A lack of engagement of supervisors (however, improved teacher/ supervisor support was only sighted by 1 student in the student survey as an area for improvement to the course, and most students in the student survey agreed that their supervision meetings provided useful guidance and feedback).

— A misunderstanding of the course focus and content, such as believing it would be a coding course.

The evidence obtained through the focus group with teachers, suggests that some of the reasons given by CIISec as to why students may drop out of the CyberEPQ, may not be applicable in all circumstances, depending on the approach to the provision of the CyberEPQ within educational institutions.

There were broadly two approaches to provision of CyberEPQ noted by teachers in the focus group, with mixed views about their effectiveness:

— First, where students were given time to complete the learning in their timetable with a member of staff being present in the class. This was considered to work well as it was made to feel like a timetabled commitment and there was concern from one teacher that students may "drift" if left to complete the learning independently. It was also a way to make sure the teacher had time dedicated to supporting the delivery of the CyberEPQ.

— Second where there was no timetabled time for either the students or teacher, with the students having to undertake the learning independently, and the teacher providing drop-in sessions at certain points to help students or being available as needed to help students. One teacher said that being able to offer the CyberEPQ without lesson time was seen as a positive aspect of the qualification for some students. However, in the teacher survey the lack of time for students to complete the CyberEPQ due to timetables was cited as a challenge by 6 out of 16 respondents (38%), and the lack of supervisor time due to workload was the most frequently cited challenge, reported by 7 out of 16 respondents (44%). One teacher in the focus group said that they needed to demonstrate the value of the CyberEPQ in order to secure time within timetables for learning.

From the students' perspective, evidence is limited as there were no respondents to the student survey who had dropped out of the CyberEPQ. However, a student who was interviewed as part of this study noted that they were told that although the CyberEPQ was free of charge for them to take, if they dropped out they would incur a £34 cost. CIISec confirmed that if a student drops out of the CyberEPQ then the school needs to pay CIISec the City & Guilds registration fee (as agreed in the funding agreement between schools and CIISec). However, it is at the discretion of the schools as to whether they ask their students to pay this fee or if it is paid from the school budget. If students face this penalty if they drop out, then this may act as a disincentive to drop out and hence encourage completion of the course. But it is unclear to what extent schools ask students to pay this fee if they drop out vs. paying it from the school budget.

Knowledge and skills

Evidence from the student survey indicates that students realised a range of benefits from taking the CyberEPQ. As shown in Figure 2 below, the most frequently reported benefits were: improved research skills (reported by 13 out of 16 student respondents (81%)); improved knowledge of the topics covered (reported by 12 student respondents (75%); and improved cyber security skills and improved ability to learn independently (each reported by 11 student respondents (69%)).

Figure 2: Benefits to students of the CyberEPQ
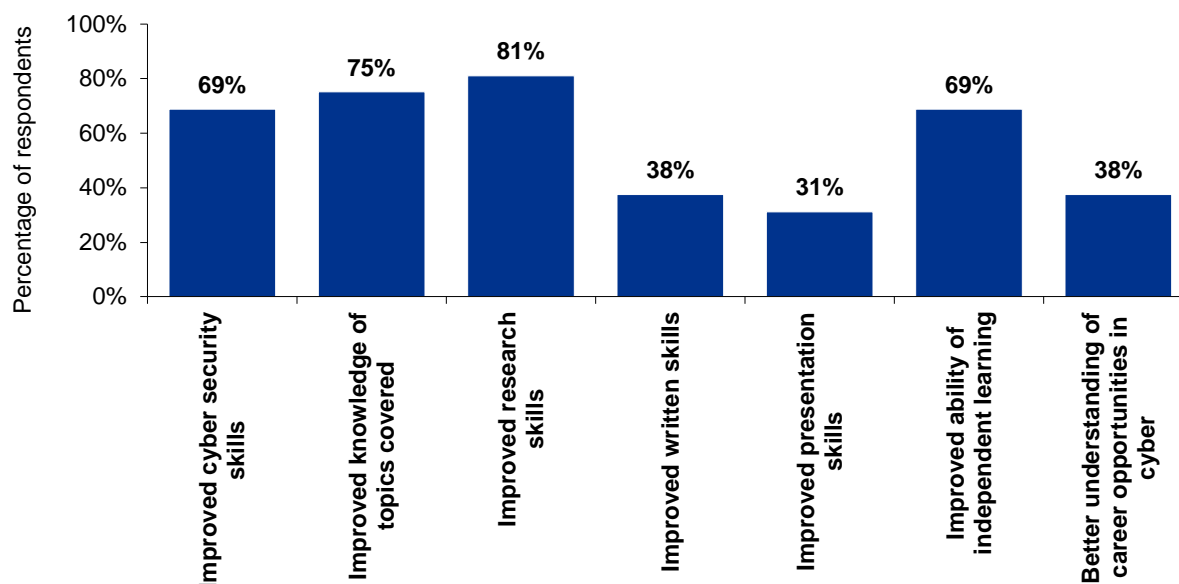
Source: KPMG analysis of student survey, 2025

Through the interviews and focus groups, further evidence was gathered on the benefits to students of completing the CyberEPQ.

In line with the survey results, research skills was a frequently cited benefit. For example, one student interviewed described how learning about research, report writing and referencing in year 12 was valuable for the coursework they then completed for English A level in year 13, and they therefore felt they were at an advantage having taken the CyberEPQ. The same student also mentioned that through speaking to experts for their research project the CyberEPQ had helped develop their interview skills.

While no student survey respondents reported "improved networks/ connections with potential employers in the cyber sector" as a benefit from taking the CyberEPQ, one student interviewed said that they anticipate further networking opportunities in the longer term from CIISec.

A small number of students interviewed also highlighted having improved their own cyber security practices having gained knowledge through the CyberEPQ. Examples given included rejecting cookies more often because of the understanding they gained of the associated risks, using VPNs instead of public Wi-Fi, and being more cautious about the information they provide online due to greater awareness about the way consumers are "manipulated" into providing information, such as pet names that are also used for security questions.

In addition to the benefits from taking the CyberEPQ noted above, the results of the student survey indicate that students developed transferable skills which they consider will be useful in their future studies and careers. As shown in Figure 3 below:

— 10 out of 14 students[24] (71%) agreed[25] with the statement "The skills I gained from the CyberEPQ course will be useful in my future career"

— 11 out of 14 students (79%) agreed[26] with the statement "The skills I gained from the CyberEPQ course will be useful in my future studies"

Figure 3: Percentage of students agreeing or disagreeing with statements about the influence of CyberEPQ
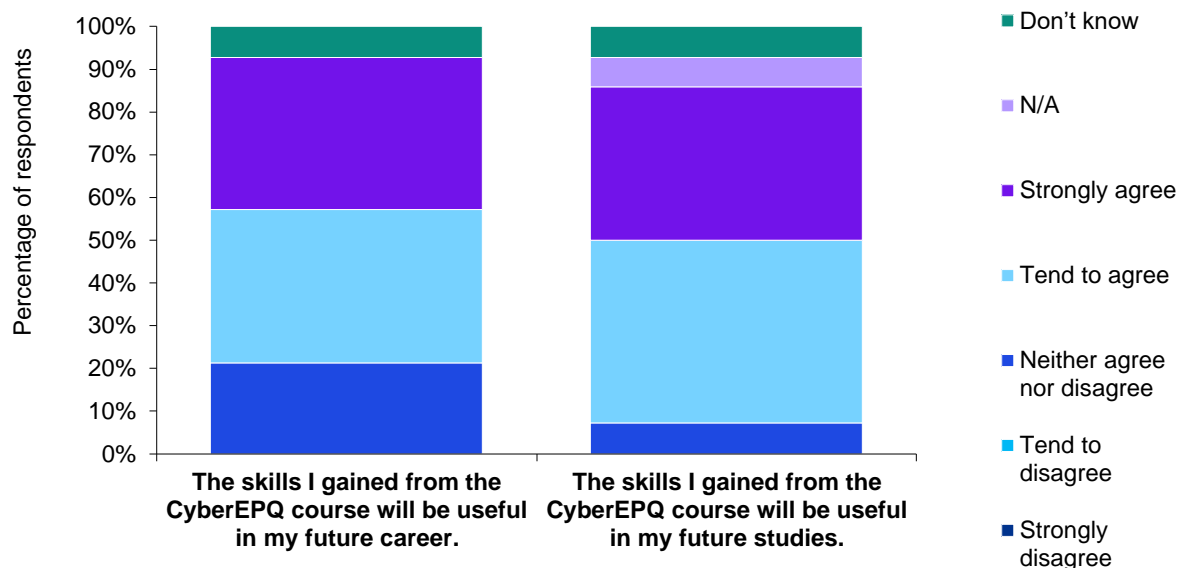
Source: KPMG analysis of student survey, 2025

Across all topic areas covered in the CyberEPQ, over half of student respondents to the student survey said that their knowledge/ skills had improved to a moderate or great extent. However, the following topic areas in the CyberEPQ were most frequently reported by students as areas where their knowledge/ skills had not improved at all or only to a small extent:

— Security Audit, Compliance & Assurance where 1 out of 16 students (6%) said their knowledge/ skills had not improved at all and 6 students (38%) said it had improved to a small extent

— Security Testing & Vulnerability Assessment where 2 out of 16 students (13%) said their knowledge/ skills had not improved at all and 4 students (25%) said it had improved to a small extent

— The History of Computing & Cryptography where 6 students (38%) said their knowledge/ skills had improved to a small extent

The benefits that students reported having gained from taking the CyberEPQ in the student survey and the interviews were somewhat consistent with the perceived benefits that CIISec and teachers mentioned in the interview and focus group respectively. CIISec and teachers both considered that CyberEPQ helped to improve the knowledge and skills of students, in particular through supporting students to learn transferable skills which prepare students for further study and to develop broad cyber security knowledge. One teacher noted that the skills developed through the CyberEPQ such as research, essay writing and presentation skills were particularly important for the types of students taking the CyberEPQ as these students were, in general, studying maths and science subjects which don't provide the same opportunity to develop these skills at A level.

---

[24] Only 14 students answered this question suggesting some students dropped out and didn't complete the survey.
[25] This includes students reporting they 'tend to agree' and 'strongly agree'.
[26] This includes students reporting they 'tend to agree' and 'strongly agree'.

In addition to knowledge and skills, both CIISec and teachers shared a number of benefits that they believe students gain from taking the CyberEPQ.

CIISec considered that students benefit in terms of:

— building networks, outside of school, with peers experiencing the same learning journey through CyberEPQ;

— personal development;

— obtaining post nominals on successful completion of the course; and

— gaining a greater appreciation that cyber security is important for all careers.

Teachers in the focus group said they perceived students benefitted in terms of:

— developing their confidence, including in applying for cyber related competitions and other opportunities (this was echoed by students in the student survey where students agreed that they felt more confident pursuing further study or a related career because of the CyberEPQ)[27]; and

— gaining increased awareness of the need for cyber security in the real world.

In terms of what could be done to improve the delivery of the CyberEPQ course to make it more effective in building students' knowledge and skills, the most frequent responses in the student survey were "more practical examples and case studies" cited by 8 out of 15 students (53%), and "improved online resources" cited by 7 out of 15 students (47%). In the interviews with students, further suggestions included:

— more interactive elements in the online delivery of modules as it was sometimes hard to absorb all the information provided in the videos; and

— additional checks to confirm learning as one student said that the answers to the multiple-choice questions at the end of compulsory modules were often common sense and they could just be clicked through and answered again if they were answered incorrectly (although the other student interviewed thought these questions were a good way of checking they had absorbed the information).

Interest in studying cyber security

A key objective of the CyberEPQ is to encourage students to undertake further, more advanced, study in cyber security after completing the qualification.

Some teachers in the focus group considered that the students taking the CyberEPQ were those that already had an interest in computing or cyber security and already had planned to pursue further study in this area. They, therefore, noted it was difficult to say that it was the CyberEPQ that had helped develop a student's interest in studying cyber security or computing further. One teacher said that the benefit of CyberEPQ was that it enabled students to test whether they enjoyed cyber security so that they could be more certain about deciding to pursue further study or a cyber security career. CIISec however, thought that students sometimes surprise themselves with what they are interested in and therefore may consider studying cyber security as a result of taking the CyberEPQ which they may not have otherwise done. This presumes, however, that students were not necessarily interested in cyber security before taking the CyberEPQ.

The responses to the student survey provide a clearer indication of students' actual intentions to undertake additional studies in cyber security and related subjects and the extent to which this had been influenced by taking the CyberEPQ.

As shown in Figure 4 below, around half of student survey respondents reported that studying cyber security, computing or a different subject at university is not part of their future plans. However, the

---

[27] 9 out of 14 respondents in the student survey agreed with the statement "I feel more confident to pursue a career in cyber security because of the CyberEPQ" and 9 out of 14 agreed with the statement "I feel more confident to pursue studying computing or a cyber-related course because of the CyberEPQ".

results of the student survey suggest that for some students the CyberEPQ had influenced their future study plans:

— 6 out of 15 student respondents (40%) said that taking the CyberEPQ had increased the likelihood of them studying cyber security at university (either to a small, moderate or great extent), and

— 4 out of 15 student respondents (27%) said that it had increased the likelihood of them studying computing at university.

— But there is also a proportion of students that reported the CyberEPQ had no impact:

— 1 student out of 15 (7%) said it had no impact on their plan to study cyber security at university as this was always what they were intending to do; and

— 4 students out of 15 (27%) said it had no impact on their plan to study computing at university as this was always what they were intending to do.

While there is evidence that for some students the CyberEPQ increased the likelihood of them studying cyber security at university, some of these student respondents also reported that taking the CyberEPQ had influenced the likelihood of them studying computing and/ or a different subject at university. At this stage, it is not known what the students ultimately went on to study.

Figure 4: Impact of the CyberEPQ on cyber security study – To what extent has taking the CyberEPQ course increased the likelihood of…
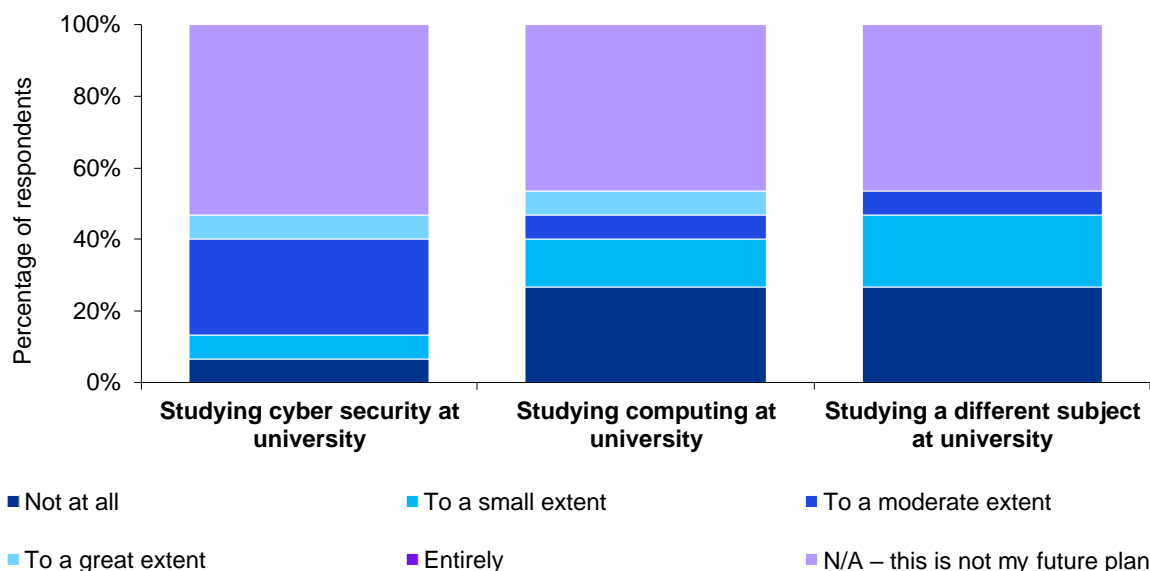
Source: KPMG analysis of student survey, 2025

A similar mixed picture emerges when looking at the extent to which students agreed with the statement, "The CyberEPQ course has made me want to pursue studying computing or a cyber-related course". 4 out of 14 students (29%) said this was not applicable to them, 1 out of 14 students (7%) strongly disagree, and 6 students (43%) agree (including tend to agree or strongly agree). In addition, while 9 out of 14 students (64%) agree (including tend to agree or strongly agree) that they "feel more confident to pursue studying computing or a cyber-related course because of the CyberEPQ", 3 out of 14 students (21%) neither agree nor disagree, but 0 students disagree.[28]

Some teachers in the focus groups noted that some students had been offered places at universities partly because of their CyberEPQ qualification, or that students received reduced offers from universities because of having the CyberEPQ qualification (the reduced offers from universities was one of the reasons a student interviewed mentioned as being a motivating factor in them taking the course). Teachers said this was because the CyberEPQ qualification acted as a differentiator and

---

[28] 2 students reported this was not applicable to them.

enabled students to compete with students from other schools with more resources who may have a more established cyber learning offer provided for students from a younger age. This is consistent with the view shared by CIISec that the CyberEPQ prepares students for further study in terms of knowledge and study skills because of the course content and delivery model. CIISec shared that it is able to support students with an interest in studying cyber security by sign-posting students to what CIISec's 40+ academic partners are offering in terms of cyber security courses.

Interest in pursuing cyber security careers

Similar to the impact of the CyberEPQ on students' interest in studying cyber security further, the results of the student survey suggest that for some students the CyberEPQ had influenced their future career plans, but for others it had no impact. As shown Figure 5 below, while 4 out of 15 students (27%) responded that it was not their future plan to seek a career in cyber security or computing, 9 out of 15 student respondents (60%) said that taking the CyberEPQ had increased the likelihood of them seeking a career in cyber security (either to a small, moderate or great extent), and 8 out of 15 student respondents (53%) said that it had increased the likelihood of them seeking a career in computing (either to a small, moderate or great extent). However, for some students this was always what they were intending to do and therefore the CyberEPQ had no influence.

While there is evidence that for some students the CyberEPQ increased the likelihood of them pursuing cyber security careers, some of these student respondents also reported that taking the CyberEPQ had influenced the likelihood of them pursuing computing careers and/ or computing apprenticeships or apprenticeships in different subjects. At this stage, it is not known what the students ultimately went on/ will go on to do.

Figure 5: Impact of the CyberEPQ on cyber security careers – To what extent has taking the CyberEPQ course increased the likelihood of…
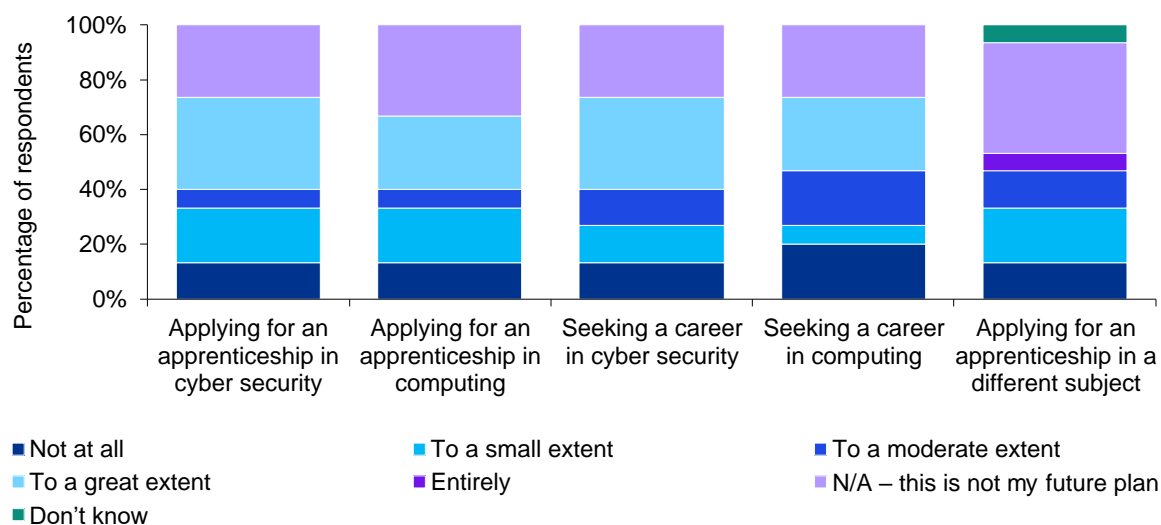
Source: KPMG analysis of student survey, 2025

A similar mixed picture emerges when looking at the extent to which students agreed with the statement, "The CyberEPQ course has made me want to pursue a career in the cyber sector". 4 out of 14 students (29%) disagree with this statement (including strongly disagree or tend to disagree), while 7 out of 14 students (50%) agree (including tend to agree or strongly agree).[29]

In addition, 9 out of 14 student respondents (64%) agreed (including tend to agree or strongly agree) that they "feel more confident to pursue a career in cyber security because of the CyberEPQ", while 2 out of 14 students (14%) disagreed (including strongly disagree or tend to disagree).[30] One of the

---

[29] 2 students reported this was not applicable to them, and 1 student reported to neither agree nor disagree.
[30] 2 students reported this was not applicable to them, and 1 student reported to neither agree nor disagree.

students interviewed said that while they currently work in education, they may move into a job in cyber security as the course has given them the reassurance and confidence to do so.

At this stage it is too early to evidence whether students who took the CyberEPQ in 2023/24 will ultimately pursue careers in cyber security. However, teachers in the focus group said that students had successfully applied to competitive apprenticeships partly because of their CyberEPQ qualification, including with Deloitte and Microsoft. Teachers said this was because the CyberEPQ qualification acted as a differentiator for students and was also something students could talk about in interviews. One teacher said that a student had used the CyberEPQ alumni network to secure a job and another said that given the vocational nature of the CyberEPQ they expect a high proportion of students will continue into the cyber security workforce.

As previously noted, some teachers participating in the focus groups considered that the students taking the CyberEPQ were those that already had an interest in cyber security careers. Therefore, they considered it was difficult to determine if it was the CyberEPQ that had helped develop students' interest in cyber security careers. One teacher acknowledged though that while this may be the case, the CyberEPQ can help to reaffirm to students the accessibility of cyber security as a career option.

CIISec also considered that the CyberEPQ may have helped students' interest in future careers in cyber security in the following ways:

— It makes students aware of jobs in the sector they may not have been aware of if they hadn't taken the CyberEPQ, which in turn can give them a career to aim towards. This is consistent with the results of the student survey where 6 out of 16 student respondents (38%) said that taking the CyberEPQ had given them a better understanding of career opportunities in the cyber sector.

— Through alumni students delivering webinars to talk about their career paths it incentivises students to pursue careers in the sector.

The students that were interviewed both mentioned that the CyberEPQ career events/ career events that CIISec advertised to them were useful in developing their understanding about employment opportunities in cyber security. In particular, they said it was useful and interesting to hear from people working in industry.

In terms of other courses available that may be perceived as comparable to the CyberEPQ, both of the students interviewed said they were not aware of anything comparable. While one student mentioned other courses that were available, none had the "prestige" associated with the CyberEPQ, or resulted in a qualification. This suggests that CyberEPQ may be providing something that is not available elsewhere, and therefore impacts realised from the CyberEPQ may not materialise in the absence of the provision of the CyberEPQ.

3.3   Effectiveness in meeting the grant objectives

The three agreed objectives for the funding from DSIT to support the delivery of the CyberEPQ were:

— to enrol students from diverse and geographically spread backgrounds at a cost of £200 per student;
— to build industry partnerships and match funding to make the CyberEPQ more financially sustainable; and
— to update the content on the online learning platform.

However, no target figures were set for any of these. The effectiveness in meeting these grant objectives are each considered in turn below.

Achieving diversity in enrolments:

One of the agreed deliverables for the grant funding from DSIT was for CIISec to "enrol students from diverse and geographically spread backgrounds". The monitoring data indicates that the students taking funded places for the CyberEPQ are not fully representative of the UK student population.

The data available on diversity is based on the number of final submissions (i.e. the research projects delivered as part of the CyberEPQ), rather than enrolments. This is the way the data is available because enrolment can take place at different points throughout the year, while there is only one point of final project submission. There were 173 submissions in 2023/24 of which:[31]

— 121 were students who received a funded place on the CyberEPQ course; and

— 43 out of 173 (25%) were female students.

Figure 6 below shows the geographical distribution of students for the 173 students that made submissions in 2023/24. As can be seen, the distribution of students is not geographically spread across the UK. For example, the highest proportion of students (23%) came from the West of England, followed by 19% from Greater London and 17% from West Yorkshire, while no students were from Tees Valley.

Figure 6: Geographical distribution of students submitting 2023/24
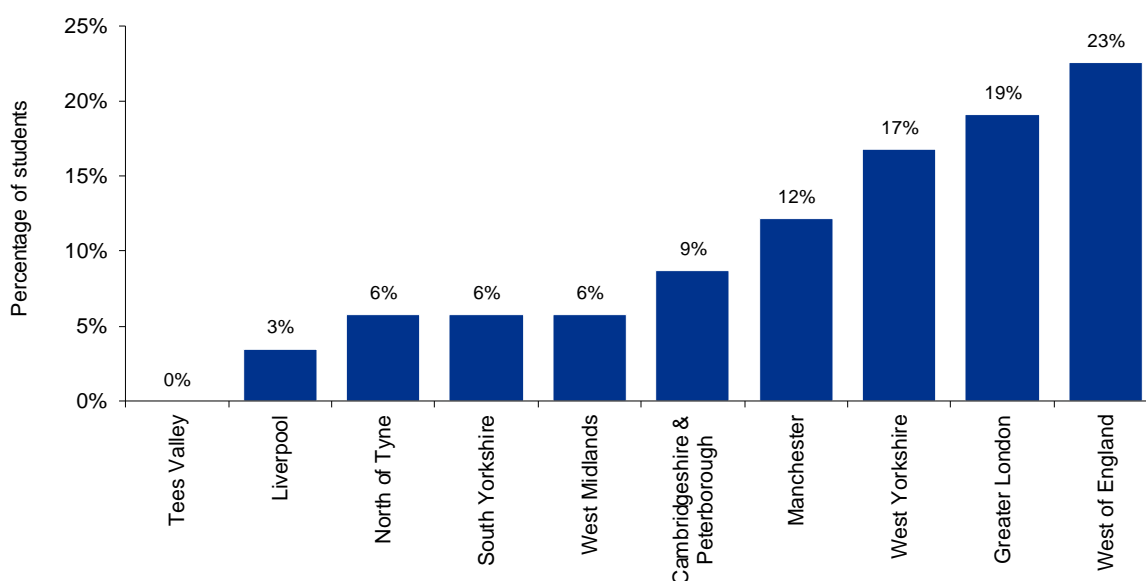
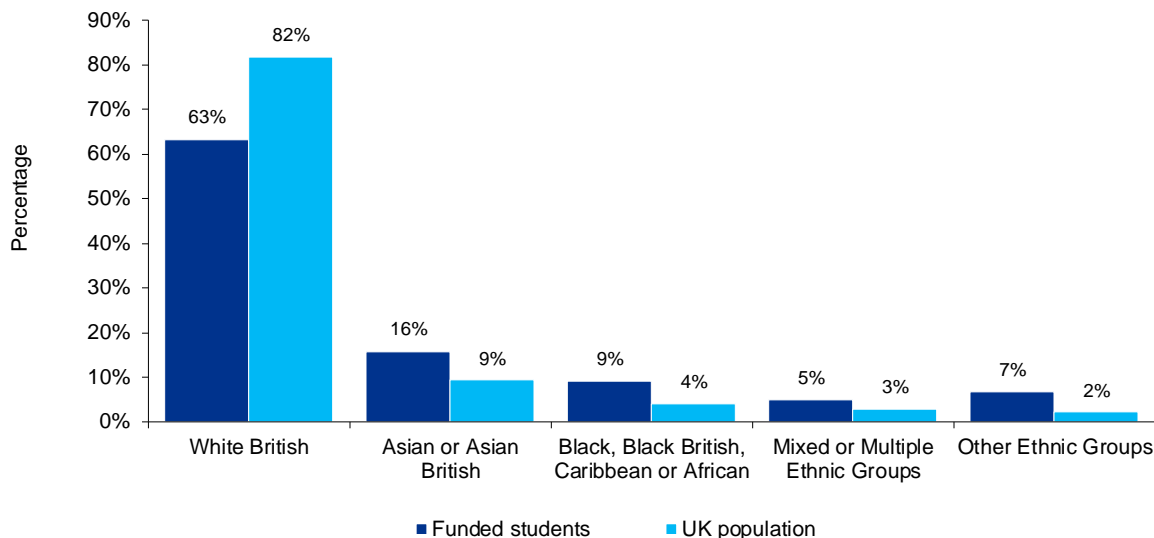

Source: CIISec data; KPMG analysis

Figure 7 below shows the ethnicity of the 120 funded students that made submissions in 2023/24, that data is available for, compared to the UK population.[32] As can be seen, the predominant ethnic group of students was White British (63% vs. 82% of the UK population), followed by 16% Asian or Asian British (compared to 9% of the UK population), 9% Black, Black British, Caribbean or African (compared to 4% of the UK population), 5% Mixed or Multiple Ethnic Groups (compared to 3% of the UK population) and 7% Other Ethnic Groups (compared to 2% of the UK population).

---

[31] CIISec CyberEPQ: 2023-2024 Overview of Activities, Summary & Reflection
[32] This is used as a proxy for the ethnicity of students for the purposes of comparison with students taking the CyberEPQ.

Figure 7: Ethnicity of funded students compared to UK population

Source: CIISec data; KPMG analysis

CIISec stated that they try to achieve diversity in enrolments in a variety of ways such as by:

— making clear to teachers that the CyberEPQ should be made available to everyone, not just students taking computing (this point was echoed by a student in an interview who considered that making the course available to all students and not just those taking computer science would encourage participation across a broader range of students);

— having specific materials for girls to advertise the CyberEPQ course, and having non-technical materials to try to dispel any myths or misconceptions about cyber security;

— trying to keep students in year 9 who take the Headstart[33] course engaged through practical cyber security-related activities such that they subsequently take the CyberEPQ in sixth form; and

— offering the Headstart course to teachers as CPD (Continuing Professional Development) to encourage them to think about offering cyber security-related courses to their students.

Teachers in the focus groups also noted the challenges in achieving diversity in enrolments, particularly in terms of increasing the number and proportion of female students taking the CyberEPQ. One teacher said that this was part of the wider issue of encouraging girls to study STEM (Science, Technology, Engineering and Maths) subjects. A number of ideas were suggested that could help encourage participation among female students, including:

— Trying to grow their interest in cyber from an earlier age, such as through the CyberFirst girls competition for year 8 or 9[34] and cyber escape rooms.

— Providing classroom time for students to study for the CyberEPQ, together with a female teacher to act as a role model, as one teacher said they believed female students preferred classroom delivery rather than independent learning.

— Emphasising the core skills that can be obtained from studying for the CyberEPQ, as one teacher said that computer science was perceived as a tech based subject, while the CyberEPQ is not perceived in this way.

One student interviewed said that a broader range of students could be encouraged to take the course if the benefits in terms of "what doors it can open" were explained, such as through examples of what past students had gone on to do.

---

[33] Headstart - CIISec
[34] CyberFirst Girls Competition - NCSC.GOV.UK

Building industry partnerships and developing match funding:

There was no specific target set in relation to this grant objective, and there was no data available/ provided on the number of industry partners developed in 2023/24 or the amount of matched funding obtained to assess performance against this grant objective. However, CIISec said that they had not delivered on the grant objective "to build industry partnerships and match funding to make the CyberEPQ more financially sustainable" in 2023/24.

CIISec said that one of the barriers to meeting this grant objective is that CIISec is not a charity, therefore corporate organisations are not simply able to "donate" money and it prevents "bulk" contributions.

However, CIISec reported that some progress since 2023/24 has been made to raise additional match funding. A key action taken by CIISec is to change the approach to obtaining sponsorship for CyberEPQ students from its corporate members. Previously, corporate members were asked to 'opt in' to sponsoring students. Now, corporate members are asked to 'opt out' of sponsoring students which has increased the number of sponsored students for CyberEPQ. Smaller organisations are defaulted to sponsoring one student, with £200 being added to their membership bill, while larger organisations are defaulted to sponsoring two students, with £400 being added to their membership bill.

In addition, CIISec reported that corporate sponsorship opportunities have been added to CIISec's website, although it is unclear what impact, if any, this has had so far. Furthermore, CIISec mentioned that there was a new person leading on building industry partnerships within CIISec, and the hope is that they will bring new ideas to build industry partnerships.

Adding new content to the online learning platform:

As explained in section 1.1, the CyberEPQ is delivered via an online learning platform (the 'Moodle'). This is where the compulsory modules are hosted together with videos, quizzes, games and downloadable resources. While it is a grant objective to add new content, no targets are set in terms of the volume of content or in relation to what it should cover.

In September 2024 new content was introduced on the online learning platform to cover two new topic areas: AI and quantum. CIISec said that these subject areas were introduced because they are evolving topic areas with growing interest, and were not covered by the course already. In addition, it was expected that there was demand to learn about these areas from students as indicated by the research project proposals submitted by students[35] which were related to these areas.

Teachers in the focus group were generally positive about the content in the online learning platform. In particular, some teachers said that the new modules were particularly good and had received positive feedback from students. One teacher noted that CIISec could be reactive to current trends in a way exam boards are not able to be.

3.4 Unintended consequences of the CyberEPQ

Neither CIISec nor teachers generally thought there had been any unintended consequences – either positive or negative – of the CyberEPQ. CIISec said that because the CyberEPQ has been delivered in a similar way since 2016, there is less likelihood of unintended consequences arising now. One teacher mentioned that as a result of offering the CyberEPQ to students, a member of staff also wanted to do the course which was seen as a positive impact, and another teacher said that offering the CyberEPQ was a unique selling point for the school, as others in the area did not offer it.

---

[35] A key part of the CyberEPQ is an independent research report carried out by students.

3.5   Challenges and areas for improvement

Through the analysis of the primary and secondar data the following areas were identified as challenges and where there is scope for improvement.

Interaction with CIISec: All teachers in the focus group agreed that the support they received from CIISec to help them deliver the CyberEPQ was effective and useful. This is consistent with the results of the Supervisor survey conducted by CIISec where 80% of respondents said they strongly agreed with the statements "I was satisfied that with the level of support, guidance and feedback received from CIISec during the CyberEPQ".[36],[37] Teachers in the focus group noted the speed at which CIISec responded to their queries as well as the support provided by CIISec more broadly to students, such as in assisting them with finding relevant research for their projects. In addition to the support received from CIISec, teachers said the other sources of support, such as the support course available on the online learning platform was also effective. In terms of areas for improvement, one teacher said that the process for data gathering by CIISec (whereby CIISec request information about the students taking the CyberEPQ and predicted grades) could be improved, such as by asking for the information upfront.

Senior leadership support: Some teachers in the focus group mentioned the challenge in persuading senior leadership of their schools to offer the CyberEPQ and there was a need to demonstrate the benefits of the qualification in order to try to secure dedicated classroom time for students to undertake the learning. This was echoed in the teacher survey where 5 out of 16 respondents (31%) cited lack of senior leadership support as a challenge, and where 5 out of 13 respondents (38%) cited that having materials to share with school senior leadership would support delivery of the CyberEPQ.

Funding: All teachers in the focus group agreed that it would be difficult to deliver the CyberEPQ without the funded places. In the Supervisor survey conducted by CIISec 17% of supervisors said they would still participate in the CyberEPQ without DSIT funding at £200 per student.[38] One teacher in the focus group said that even part funding would help to enable delivery of the CyberEPQ. Uncertainty around future funding was considered a challenge by one teacher as it prevented them being able to plan for the future, such as advertising the CyberEPQ. The qualification cost was considered a barrier by 6 out of 16 respondents (38%) to the teacher survey.

Industry interaction: Teachers in the focus group said that interaction with people working in the cyber security industry is very positive for students. Different channels for this interaction were suggested as ways to improve the CyberEPQ. Teachers said that the CyberEPQ could be improved by including work experience opportunities for students, either virtually or in-person, as it can be difficult for students to secure good quality work experience. In addition, teachers said that CIISec has lots of connections that could be used to invite professionals to speak to students.

3.6   Concluding remarks

This study aims to answer the specific research questions agreed with DSIT at the outset and is therefore narrower in scope than a full evaluation. The analysis suggests that while the CyberEPQ has been effective in building some student's interest in studying cyber security and pursuing careers in cyber security, this is not the case for all students. Some students already had planned to do this. However, the evidence indicates that students realised a range of benefits from taking the CyberEPQ including developing knowledge and skills related to cyber security, but also broader, transferable skills.

---

[36] With the remaining respondents saying they agreed with this statement.
[37] CIISec CyberEPQ: 2023-2024 Overview of Activities, Summary & Reflection
[38] CIISec CyberEPQ: 2023-2024 Overview of Activities, Summary & Reflection

www.kpmg.com/uk

Use of this report is limited – see Important notice