Evaluation of the Cyber Skills Immediate Impact Fund Pilot

Department for Digital, Culture, Media and Sport (DCMS)

September 2020

Fieldwork period January – March 2019
Report completed July 2019

CONTENTS

Disclaimer:

The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made.

Recommendations for improvements should be assessed by you for their full impact before they are implemented. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

This report is supplied on the understanding that it is solely for the use of the persons to whom it is addressed and for the purposes set out herein. Our work has been undertaken solely to prepare this report and state those matters that we have agreed to state to them. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM UK Consulting LLP for any purpose or in any context. Any party other than the Board which obtains access to this report or a copy and chooses to rely on this report (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM UK Consulting LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to our Client on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

We have no responsibility to update this report for events and circumstances occurring after the date of this report. RSM UK Consulting LLP is a limited liability partnership registered in England and Wales no. OC397475 at 6th floor, 25 Farringdon Street, London EC4A 4AB

EXECUTIVE SUMMARY

RSM UK Consulting LLP (RSM) was commissioned by the Department for Digital, Culture, Media and Sport (DCMS) to evaluate its Cyber Skills Immediate Impact Fund (CSIIF) pilot against the following research questions:

1. Is CSIIF an effective form of government intervention that succeeds in its aim of stimulating the market to build an immediate route into the cyber security talent pipeline?
2. Are the sponsored projects an effective method (for the candidate, the employer and the market) of retraining and upskilling candidates in the immediate term for an entry-level cyber security role?

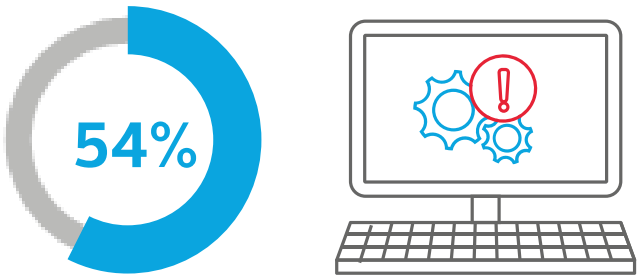
The methodology for this evaluation included: desk research; consultations with DCMS representatives, representatives from the 7 funded providers and 2 sector representatives; surveys of people who took part in the pilot (beneficiaries) and people who applied to take part in the pilot but were unsuccessful (control group). This report presents the findings of the evaluation.

In line with rules around disclosure of funding amounts under the National Cyber Security Programme some financial information, including assessment of value for money, is not included in this published version.

Why was government intervention needed?

The government aims to develop the UK cyber security sector.[1] However, a review of the literature indicates the following market failures:

- **cyber security skills gap** - more than half of all UK businesses have a basic cyber security skills gap[2]
- **lack of awareness of career opportunities and perceptions of the industry** as male dominated[3] and 'geeky'[4] reduces the number of people entering the sector



54% of UK businesses have a basic cyber security skills gap

[1] *HM Government (2016) National Cyber Security Strategy 2016 – 2021, HM Government (2018) Initial National Cyber Security Skills Strategy: increasing the UK's cyber security capability - a call for views [online] available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/767515/Cyber_security_skills_strategy_211218.pdf [accessed 01/04/19] and HM Government (2017) UK Digital Strategy*

[2] *Ipsos Mori (2018) Understanding the UK Cyber Security Skills Labour Market https://www.ipsos.com/sites/default/files/ct/publication/documents/2019-01/understanding_the_uk_cyber_security_skills_labour_market.pdf [accessed 08/05/19]*

[3] *Kaspersky Lab (2017) Beyond 11%: A study into why women are not entering cybersecurity. [online]. Available at: https://d1srlirzdlmpew.cloudfront.net/wp-content/uploads/sites/86/2017/11/03114046/Beyond-11-percent-Futureproofing-Report-EN-FINAL.pdf [Accessed 15/02/2019].*

[4] *Dallaway, E. (2017) closing the gender gap in cyber security, United Kingdom: CREST. [online]. available at: https://www.crest-approved.org/wp-content/uploads/CREST-Closing-the-Gender-Gap-in-Cyber-Security.pdf [accessed 03/06/2019].*

There is also a **lack of diversity** in the sector[5], caused by barriers affecting specific groups, such as:

- women – *the relatively low* ***proportion of women in the industry and studying related subjects[6] limits the supply of suitable candidates***
- neurodiverse people - *traditional* ***recruitment practices*** *can be a barrier to employment for this group[7]*

This limits the flow of UK talent into the cyber security profession and confirms the need for government interventions to boost the volume and diversity of people transitioning into entry-level cyber security jobs.

CSIIF has been designed to create more entry-level skilled people coming from a range of diverse backgrounds and therefore has the potential to contribute to the current government strategies[8] for cyber security skills.

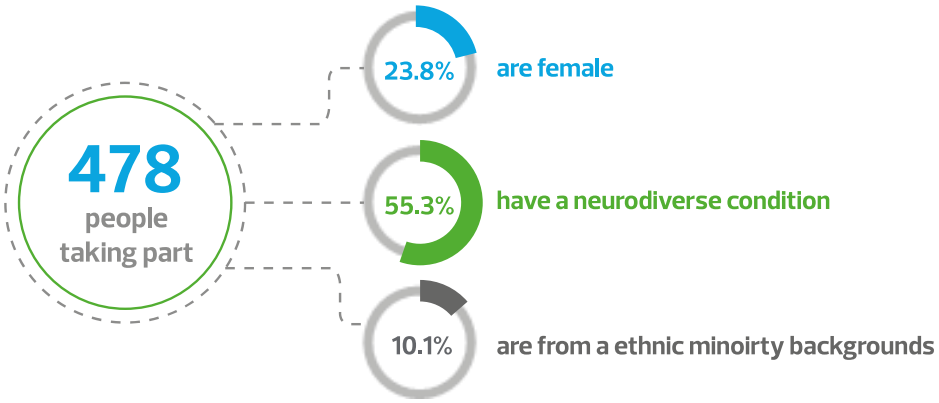
What was the intervention?

The CSIIF pilot:

- aimed to develop the pipeline of UK cyber security talent by training individuals, not currently engaged in the sector, for entry-level cyber security roles
- aimed to boost the diversity of the sector, particularly in relation to women and neurodiverse candidates
- provided grant funding for organisations to develop, scale up, or refocus their cyber security training projects to help equip individuals for entry-level cyber security roles within 6 months
- funded 7 projects with grant awards ranging from £20,000 to £70,000

[5] *British Computer Society (BCS) (2017) Diversity in IT 2017: shaping our future together. [online]. available at: https://www.bcs.org/upload/pdf/diversity-report-2017.pdf [accessed 28/03/19].*
[6] *Ecorys (2016) Digital Skills for the UK Economy. [online]. available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492889/DCMSDigitalSkillsReportJan2016.pdf [accessed 08/05/19].*
[7] *Partridge, R. (2018) Tapping into neurodiversity for new cyber security skills. [online]. Available at: http://www.engineeringnews.co.za/article/tapping-into-neurodiversity-for-new-cyber-security-skills-2018-06-18/rep_id:4136 [Accessed: 20/02/2019].*
[8] *HM Government (2016) National Cyber Security Strategy (2016-2021). [online]. available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf [accessed 08/05/19]; HM Government (2018) initial national cyber security skills strategy (2018). [online]. available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/767515/Cyber_security_skills_strategy_211218.pdf [accessed 01/04/19]; HM Government (2017) UK digital strategy. [online]. available at: https://www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy [accessed 08/05/19].*

What has the intervention achieved?



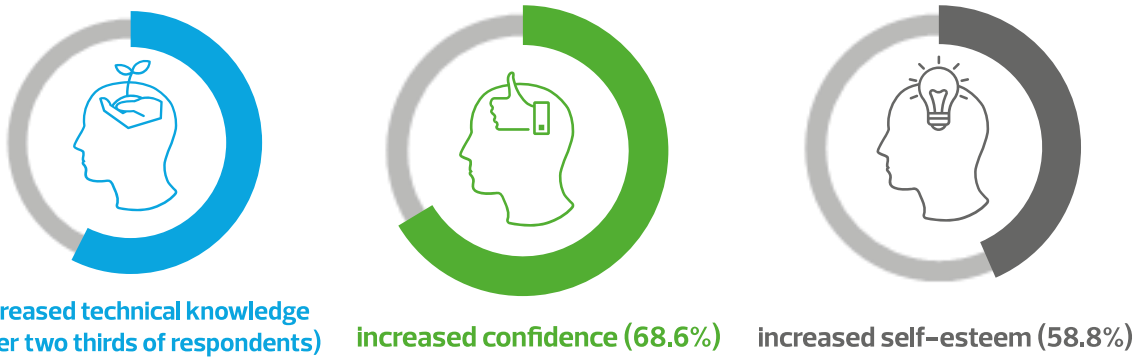
Almost 480 candidates have taken part in training initiatives funded by the CSIIF pilot to date (as of May 2019). This exceeds the overall target for the fund (by 38.2%). The pilot has achieved 89.8% of its target for the number of female candidates. The target for the number of neurodiverse candidates has been exceeded (by 68.2%). The project has been successful in attracting more diverse candidates into the sector:

- 23.8% of candidates are female
- 55.3% of candidates have a neurodiverse condition
- 10.1% of candidates are from ethnic minority backgrounds[9]

have been placed into employment

A total of 44 candidates have been placed into employment to date (as of May 2019). The majority of survey respondents (74.1%) were still completing their CSIIF training, however, they were already able to identify a range of positive outcomes, including increased technical knowledge (over two thirds of survey respondents), increased confidence (68.6%), self-esteem (58.8%) and employment outcomes (35.7% of survey respondents who had completed their training were working in cyber security). However, the low number of candidates who viewed themselves as role models for others wishing to enter the sector (17.6%) suggests that more could be done to celebrate the fact that these people are pioneers for diversity within the sector.

[9] *THIS IS BASED ON INFORMATION FROM 4 PROJECTS, THE REMAINING 3 DID NOT RECORD CANDIDATES' ETHNIC BACKGROUND*



The pilot has also exceeded its target for match funding. The total amount of match funding achieved is greater than the total CSIIF grant award[10], which is evidence of employer buy-in.[11]

There is evidence that the providers would not have been able to deliver these projects at the same scale without CSIIF funding. The estimated additionality range for the pilot is between 60% and 75%, which suggests that between 287 and 359 candidates would not have been engaged in cyber security training without the pilot and 26 to 33 candidates would not be employed in cyber security. **The bases for both surveys are low, therefore, these figures are indicative and should not be relied on.**

What lessons can be learned from CSIIF?

The pilot has successfully supported 7 organisations to develop cyber security projects, providing training for almost 480 candidates to date.

The diverse nature of the projects in terms of the target groups supported and the range of training offered, from technical skills to employability support, was viewed positively by sector representatives. It has also resulted in projects working together to create synergies.

It is the recommendation of this evaluation, therefore, that DCMS continues the fund.

How could CSIIF change to increase its impact?

Due to the current shortage of entry-level cyber security professionals, the pilot focuses on training new entrants to the sector. However, the speed of change in malware and cyber attacks highlights the need for the continued professional development of this group, to keep their skills relevant and prevent them from being overlooked in favour of newer entrants with more recent, and therefore, more relevant training.

> *Recommendation 1: Future funding opportunities should consider how government can further support ongoing training for existing entry-level professionals, as well as training provision for new entrants, to make sure that they keep up to date with changes in the sector.*

The pilot exceeded DCMS' expectations in terms of the number of successful applications from providers. The successful providers also cover a suitably broad range of target groups and training approaches. However, one sector representative felt that notifying a wider group of providers, including ones not currently engaging with DCMS, could help to encourage greater diversity.

---

[10] *In line with rules around disclosure of funding amounts under the National Cyber Security Programme some financial information, including assessment of value for money, is not included in this published version.*

[11] *This analysis is based on data collected via the CSIIF provider consultations and has not been verified by DCMS or RSM.*

Recommendation 2: DCMS should advertise future funding opportunities further in advance and with a wider group of providers to encourage more diverse proposals. This would also give providers more time to engage employers and referral agencies in the development of their proposals, resulting in them setting more informed and realistic targets and timeframes.

DCMS has verified 87% of CSIIF spend to date, but there has been no reporting or verification of match funded expenditure to date. We recommend that:

Recommendation 3: Financial reporting requirements for projects and verification of spend by DCMS includes match funded expenditure. DCMS should also ask projects to submit a declaration of match funding at least once a year.

Although 262 (54.8%) candidates have completed their training[12], only 44 candidates have been placed into employment (as of May 2019). However, this research indicates that some projects include work placements in these employment figures. Therefore, we recommend that:

Recommendation 4: DCMS establishes a clear definition of the type of employment it intends candidates to be engaged in within 6 months of completing their project.

Providers indicate that the lead in time required for some projects was longer than expected, particularly in relation to educating employers about the needs of neurodiverse candidates. We recommend that:

Recommendation 5: DCMS encourages applicants of future funds to learn from the pilot and include sufficient lead in time for employer engagement, resulting in the setting of more realistic timeframes and targets.

The full benefits of this pilot will take longer to materialise than was originally expected. DCMS should continue its support of the pilot projects to make sure that the momentum built up by its initial investment is not lost in the medium term whilst projects are securing their long-term sustainability. This support could take the form of bridge funding, where appropriate, but also employer education. One of the main challenges projects have faced is educating employers about how to support diversity and inclusion. This is an area where DCMS is well placed to intervene:

Recommendation 6: DCMS should share examples of employers who are supporting diversity and inclusion in the sector well, in addition to sharing examples of good practice and lessons learned from CSIIF on how to support the recruitment and retention of target groups.

While the pilot has resulted in a number of positive outcomes for beneficiaries, the low number of candidates who considered themselves role models for people wishing to enter the sector indicates that:

Recommendation 7: DCMS, the National Cyber Security Centre (NCSC) and CSIIF providers, could do more to reinforce the idea that the people participating in these projects are leading the diversification of the UK cyber security industry.

As noted above the full impact of the pilot will take longer to materialise, therefore:

Recommendation 8: DCMS should work with projects to gain participant consent to take part in longitudinal research into beneficiary outcomes (over the next 3 to 5 years) so that

[12] *THIS DOES NOT INCLUDE THE 193 CANDIDATES FROM IMMERSIVE LABS WHO DO NOT TECHNICALLY COMPLETE THE INITIATIVE. THESE 193 CANDIDATES HAVE COMPLETED A TOTAL OF 8,389 INDIVIDUAL LABS, EQUATING TO ROUGHLY 1,900 HOURS TRAINING.*

the full benefits of the pilot can be measured. If this was done by creating some form of CSIIF alumni group, it could also support achievement of Recommendation 7.

Is CSIIF an effective form of government interventivon that succeeds in its aim of stimulating the market to build an immediate route into the cyber security talent pipeline?

Are the sponsored projects an effective method (for the candidate, the employer and the market) of retraining and upskilling candidates in the immediate term for an entry-level cyber security role?

Do the sponsored projects represent value for money?

1. INTRODUCTION

1.1 Overview

RSM UK Consulting LLP (RSM) was commissioned by the Department for Digital, Culture, Media and Sport (DCMS), in December 2018, to evaluate its Cyber Skills Immediate Impact Fund (CSIIF) pilot. This report summarises the findings of the evaluation.

The remainder of this section outlines the terms of reference of the evaluation, the methodology used and the report structure.

In line with rules around disclosure of funding amounts under the National Cyber Security Programme some financial information, including assessment of value for money, is not included in this published version.

1.2 Terms of reference

This evaluation seeks to answer the research questions set out in the Invitation to Tender (ITT) and refined during our evaluation:

1. Is CSIIF an effective form of government intervention that succeeds in its aim of stimulating the market to build an immediate route into the cyber security talent pipeline?
2. Are the sponsored projects an effective method (for the candidate, the employer and the market) of retraining and upskilling candidates in the immediate term for an entry-level cyber security role?

1.3 Methodology

The evaluation methodology was designed by RSM to address these research questions and agreed in collaboration with DCMS. It includes the following 4 stages:

- **Stage 1: Desk research** – involving a literature review and analysis of available project and contract documentation and monitoring information. At this stage we also mapped the pilot against cyber security frameworks[13] to see whether it is focused on the main skills gaps.
- **Stage 2: Consultations** with:
  - DCMS representatives
  - representatives from all 7 providers that received CSIIF funding[14]
  - two sector representatives

[13] *THE CYBER SECURITY BODY OF KNOWLEDGE (CYBOK) AND NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) CYBER SECURITY FRAMEWORKS WERE BOTH CONSIDERED FOR THIS EVALUATION. CYBOK FOCUSES ON WHAT A PROFESSIONAL SHOULD KNOW, BUT IT IS STILL IN DEVELOPMENT. THIS RAISED CONCERNS ABOUT HOW FAMILIAR IT WOULD BE TO RESEARCH PARTICIPANTS. WE GAVE THIS FEEDBACK TO THE CYBOK TEAM. IT WAS WELL RECEIVED. NIST IS ORGANISED AROUND CYBER SECURITY TASKS, ALIGNING WELL WITH JOBS AND REINFORCED BY MANY VENDORS WHO HAVE ADOPTED CLOSE VARIANTS OF IT. THE RESEARCH INSTRUMENTS FOR THIS EVALUATION INCLUDED QUESTIONS ON IDENTIFY, PROTECT, DETECT, RESPOND AND RECOVER WHICH MAP WELL TO JOBS. WE ALSO CHOSE TO INCORPORATE THE 'HUMAN, ORGANISATIONAL AND REGULATORY' ASPECTS OF CYBOK AS THESE ASPECTS ARE LESS EXPLICIT WITHIN THE NIST FRAMEWORK.*

[14] *WE ALSO DESIGNED AN ONLINE SURVEY TO CAPTURE THE OPINIONS OF PROVIDERS WHO APPLIED FOR CSIIF FUNDING BUT WERE UNSUCCESSFUL. THE SURVEY WAS DISTRIBUTED BY DCMS TO FIVE ORGANISATIONS. ONLY ONE RESPONDED.*

- **Stage 3: Surveys of CSIIF applicants** - 2 online surveys were distributed, via the 7 CSIIF providers to:
  - people who applied to take part in the pilot and were successful (beneficiaries) - achieving 54 responses[15]
  - people who applied to take part in the pilot but were unsuccessful (control group) - achieving 20 responses[16]
- **Stage 4: Analysis and reporting** - the analysis has been shared with DCMS throughout the evaluation, in accordance with the evaluation plan. This report summarises our analysis, conclusions and recommendations for CSIIF

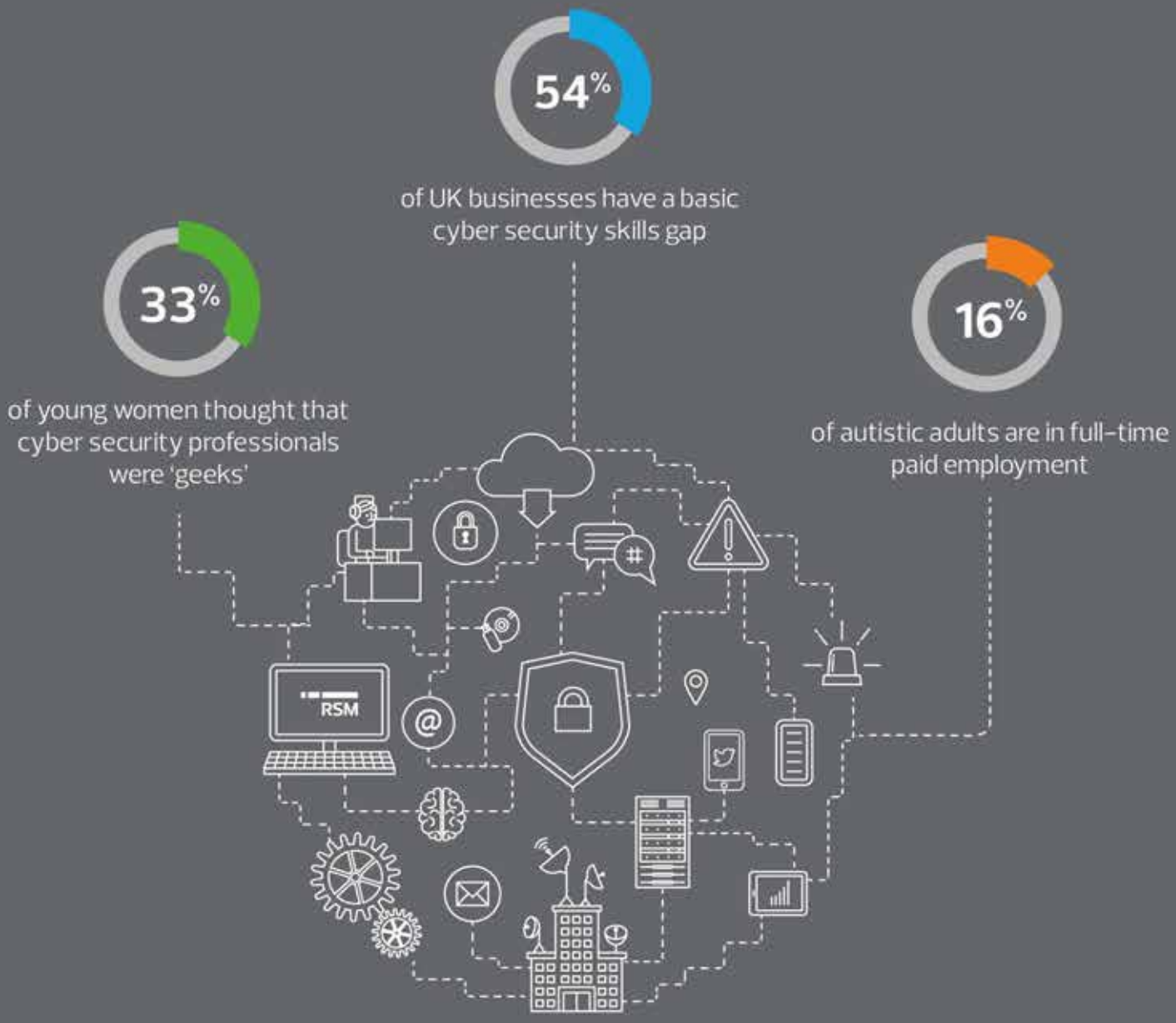
1.4 Report structure

The remainder of this report is structured under the following sections:

- Need for government intervention
- Intervention
- Performance
- Conclusions and recommendations
- Appendix A: CSIIF projects
- Appendix B: Profile of survey respondents

[15] *TOTAL POPULATION OF 285 (478 CANDIDATES LESS CANDIDATES FROM YOUTH FED (187), PGI (0) AND NAS (6)). YOUTH FED, WAS UNABLE TO DISTRIBUTE THE SURVEY LINK AS IT DOES NOT HOLD CONTACT DETAILS FOR ITS CANDIDATES. IT WAS ABLE, HOWEVER, TO SHARE FEEDBACK IT HAD COLLECTED FROM 60 CANDIDATES. DUE TO THE TIMING OF THE SURVEYS IT WAS AGREED WITH DCMS THAT CANDIDATES FROM PGI AND NAS WOULD NOT BE SURVEYED. 54 RESPONSES GIVES A RESPONSE RATE OF 18.9%, WHICH IS REASONABLE FOR AN EXTERNAL ONLINE SURVEY ADMINISTERED VIA A THIRD PARTY. HOWEVER, DUE TO THE RELATIVELY LOW POPULATION, THE MARGIN OF ERROR FOR THIS SURVEY IS RELATIVELY HIGH (± 12% AT THE 95% CONFIDENCE LEVEL). THIS MEANS THAT THE SURVEY FINDINGS ARE INDICATIVE AND SHOULD NOT BE GENERALISED TO REPRESENT THE WHOLE POPULATION.*

[16] *TOTAL POPULATION OF 34 (878 APPLICANTS TO DATE MINUS 285 CANDIDATES AND APPLICANTS FROM YOUTH FED (187), PGI (360) AND NAS (12)). 20 RESPONSES GIVES A RESPONSE RATE OF 58.8%, WHICH IS GOOD FOR AN EXTERNAL ONLINE SURVEY ADMINISTERED VIA A THIRD PARTY TO UNSUCCESSFUL APPLICANTS. HOWEVER, DUE TO THE RELATIVELY LOW POPULATION, THE MARGIN OF ERROR IS RELATIVELY HIGH (± 14% AT THE 95% CONFIDENCE LEVEL). THIS MEANS THAT OUR SURVEY FINDINGS ARE INDICATIVE AND SHOULD NOT BE GENERALISED TO REPRESENT THE WHOLE POPULATION.*


54%
of UK businesses have a basic cyber security skills gap
33%
of young women thought that cyber security professionals were 'geeks'
16%
of autistic adults are in full-time paid employment
RSM

2. NEED FOR GOVERNMENT INTERVENTION

2.1 Overview

The Chancellor announced that the government would invest £1.9 billion to protect the UK against cyber threats[17] and that part of this investment would be directed to a progressive skills programme to enhance the skills and knowledge of the UK's cyber security industry.

Working alongside the National Cyber Security Centre (NCSC) and the Cabinet Office, DCMS is responsible for implementing skills initiatives which form part of the National Cyber Security Programme (NCSP). CSIIF is one of a range of pilot initiatives being used by DCMS to test different approaches to addressing the skills shortage.[18] It was established to provide funding for organisations to develop, scale up and refocus projects that aim to get non-cyber security professionals into entry-level cyber security roles within 6 months.

The aim of this section of the report is to establish the need for government intervention. It includes the following sub headings:

- Policy context – *setting the context for the CSIIF pilot*
- Need for cyber security professionals – *describing the demand for cyber security skills in the UK*
- Need for CSIIF – *explaining how the pilot aims to address the market failures identified in the sections above*
- Summary – *presenting findings on the need for government intervention*

2.2 Policy context

The **National Cyber Security Strategy (2016-2021)** identifies the absence of established training pathways into the profession as one of the market failures leading to the cyber skills shortage.[19] One of its strategic objectives is to ensure the sustained supply of the best possible cyber security talent in the UK, whilst funding specific interventions in the short term to help meet known skills gaps. CSIIF aims to contribute to the achievement of this objective by providing effective and clear entry routes into the cyber security profession for a diverse range of people such as women and people with neurodiverse conditions.

CSIIF also has the potential to contribute to the **Initial National Cyber Security Skills Strategy (2018)**[20] strategic objective of ensuring the UK has education and training systems that provide the right building blocks to help identify, train and place new and untapped cyber security talent. It aims to do this by encouraging people to retrain for entry-level cyber security roles.

---

[17] NCSC (2017), Britain to enter 'new era of online opportunity'. [online] available at: https://www.ncsc.gov.uk/news/britain-enter-new-era-online-opportunity [accessed 22/03/2019].

[18] In line with rules around disclosure of funding amounts under the National Cyber Security Programme some financial information, including assessment of value for money, is not included in this published version.

[19] HM Government (2016) National Cyber Security Strategy (2016-2021). [online]. available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf [accessed 08/05/19];

[20] HM Government (2018) Initial National Cyber Security Skills Strategy: increasing the UK's cyber security capability - a call for views. [online]. available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/767515/Cyber_security_skills_strategy_211218.pdf [accessed 01/04/19].

The **UK Digital Strategy (2017)**[21] also highlights the need to protect the UK from cyber threats by addressing the skills shortage. It aims to achieve that by developing a self-sustaining pipeline of UK talent providing the skills to meet and overcome future threats and challenges. CSIIF will support this aim by retraining people not previously engaged in cyber roles to become cyber security professionals.

2.3 Need for cyber security professionals

A global shortfall of 3.5 million open cyber security jobs is predicted by 2021.[22] Despite the volume of cyber security breaches and attacks (43% of businesses and 19% of charities based in the UK experienced a cyber security breach or attack in the last year[23]) organisations are not well prepared:

- only 27% of businesses and 21% of charities in the UK have a formal cyber security policy[24]
- the number of professionals in specific cyber security roles is small with many absorbing the role into an existing non-cyber security job,[25] often lacking technical expertise, resulting in a relatively immature UK cyber security labour market[26]

Ipsos MORI's review of the UK cyber security skills labour market[27] demonstrates a substantial demand for basic technical skills particularly in food or hospitality and construction firms. It also shows that 90% of businesses are confident that those involved in their cyber security would be able to back up files and data, but far fewer are confident about their ability to detect and remove malware (67%), store or transfer personal data in a secure way (65%) or set up configured firewalls (59%). The study identifies a basic cyber security skills gap in over half of all businesses (54% of businesses were not confident in carrying out one or more of these basic tasks). At a national level this is equivalent to approximately 710,000 of the UK's c.1.3 million businesses.[28]

---

[21] *HM Government (2017) UK Digital Strategy. [online] available at: https://www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy [accessed 08/05/19].*

[22] *Cybersecurity Ventures (2017) Cybersecurity Jobs Report 2018-2021. [online] available at: https://cybersecurityventures.com/jobs/ [accessed 08/05/19].*

[23] *DCMS (2018) Cyber Security Breaches Survey. [online] available at: https://assets.publishing.service. gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf [accessed 03/06/2019].*

[24] *IBID*

[25] *Ipsos Mori (2018) Understanding the UK Cyber Security Skills Labour Market. [online]. available at: https://www.ipsos.com/sites/default/files/ct/publication/documents/2019-01/understanding_the_uk_cyber_security_skills_labour_market.pdf [accessed 08/05/19].*

[26] *An important caveat for these findings is that they do not specifically reflect firms in the cyber security industry itself (the ones working on cyber security technological developments, products or services) – they represent those working in cyber security roles within other industries.*

[27] *This includes analysis from a quantitative survey of 1,030 businesses, 127 public sector organisations and 470 charities from 12 June to 6 August 2018.*

[28] *Ipsos Mori (2018) Understanding the UK Cyber Security Skills Labour Market. [online]. available at: https://assets.publishing.service. gov.uk/government/uploads/system/uploads/attachment_data/file/767422/Understanding_the_UK_cyber_security_skills_labour_market.pdf [accessed 08/05/19].*

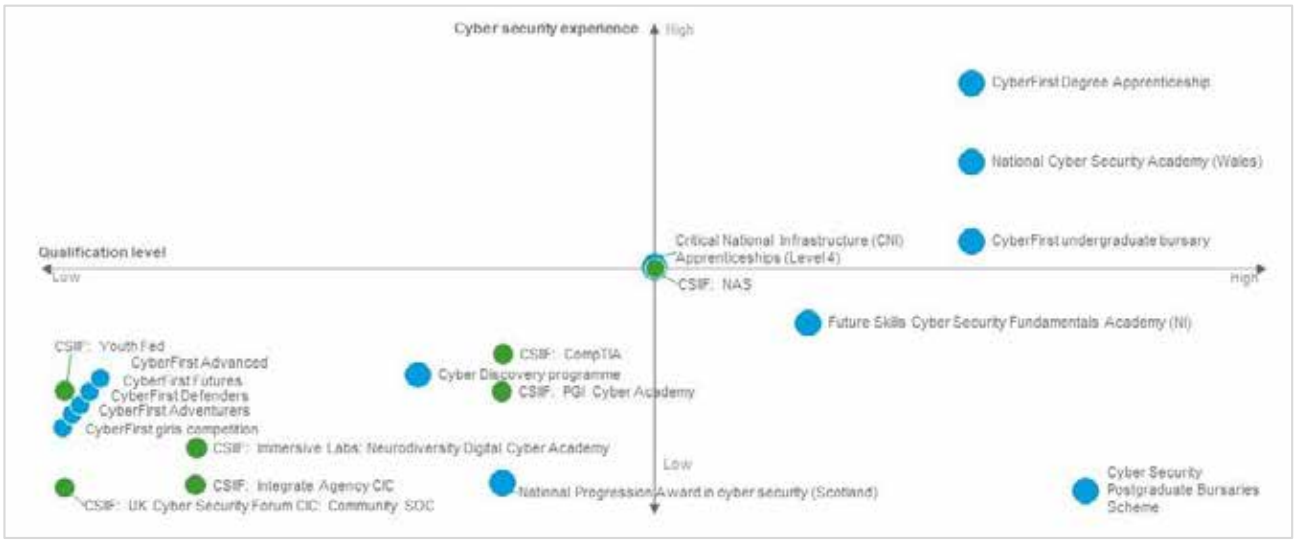
2.4 Need for CSIIF

The CSIIF pilot aims to incentivise a range of organisations to develop, scale up or refocus cyber security training projects in order to increase the volume and diversity of adults moving into entry-level cyber security jobs in the UK. The pilot also aims to help address the underrepresentation of women and neurodiverse candidates in the profession.

2.4.1 Fit with existing initiatives

CSIIF is part of a range of DCMS initiatives to pilot different approaches to help address the cyber security skills gap. Figure 2.1 is an indicative map of interventions supported by the UK Government. It includes seed-funding initiatives developed by industry as well as those sponsored by government to feed into wider sector skills requirements. The vertical axis shows the level of cyber security experience gained through the initiative in terms of time (ranging from no practical experience to job shadowing and work-based projects and placements). The horizontal axis shows the level of qualification gained (ranging from no formal qualifications to Level 8 on the national qualifications framework (PhD or DPhil)). Please note that subjective judgement has been used to determine the position, along the horizontal axis, of projects that award certificates, that do not have an equivalent qualification level.

Figure 2.1: Publicly funded cyber security training initiatives



SOURCE: RSM ANALYSIS OF THE INITIAL NATIONAL CYBER SECURITY SKILLS STRATEGY (2018)

KEY: CSIIF PROJECTS (DUE TO THE DIVERSE NATURE OF THE 7 PROJECTS FUNDED UNDER THE CSIIF PILOT THESE HAVE BEEN PRESENTED SEPARATELY AND COLOURED GREEN TO DISTINGUISH THEM FROM THE OTHER INTERVENTIONS)

OTHER INTERVENTIONS

NOTES: THE DIGITAL SCHOOLS AWARDS, SCOTLAND HAS NOT BEEN INCLUDED IN THIS DIAGRAM. IT AIMS TO HELP SCHOOLS DEVELOP THEIR DIGITAL SKILLS PROVISION FROM EARLY YEARS (NURSERY SCHOOL) THROUGH PRIMARY AND SPECIAL EDUCATION AND INTO SECONDARY LEVEL EDUCATION. THIS WOULD SPAN THE BOTTOM LEFT QUADRANT OF FIGURE 2.1.

Figure 2.1 illustrates the broad range of publicly funded interventions in terms of the experience provided and level of qualification gained. The 7 projects funded through the CSIIF pilot are in the bottom left quarter of the diagram representing relatively low levels of qualification and experience gained. They are distinct from the other initiatives in this space in that they are primarily aimed at adults, who are new to the sector. The CyberFirst initiatives, the Cyber Discovery programme and the Scottish National Progression Award in cyber security are all aimed at school children with an interest in cyber security. The Critical National Infrastructure (CNI) Apprenticeships scheme and the CSIIF funded NAS project both offer the same level of qualification and work experience, but NAS has a specific focus on people with autism. Therefore, there is no duplication between CSIIF and existing supports. The individual CSIIF projects are discussed in Section 3 and Appendix A of this report.

2.4.2 Fit of the pilot with identified skills needs

The 7 CSIIF projects aim to provide the training required to prepare candidates for immediate entry-level cyber security roles. As Figure 2.1 shows, most CSIIF projects involve a combination of knowledge development and practical experience. The 2 projects that do not include practical experience, do invite guest speakers from industry to help candidates understand how the knowledge is applied in practice.

It is reasonable, therefore, to expect CSIIF projects to improve candidates' confidence in carrying out the range of basic cyber security tasks and equip them for entry-level cyber security roles. However, as the nature of malware and attacks change, organisations will need to change the way they respond. Some basic cyber security tasks will be automated away, others will require a much deeper knowledge to be carried out effectively, and new tasks will emerge. This highlights the need for continued professional development of this group to keep their skills relevant. While the pilot focuses on new entrants to the sector, in the future, ongoing training support will be needed to ensure entry-level cyber security professionals are kept up to date with changes in the sector and prevent them from being overlooked in favour of new entrants with more recent, and therefore, more relevant training (Recommendation 1). Both sector representative bodies and employers have a role to play in ensuring entry-level cyber security professionals are adequately improving their skillset.

2.4.3 Helping deliver a more diverse workforce

One of the goals of the National Cyber Security Strategy is to address the lack of diversity within the cyber security sector. This includes not only gender, but ethnic, neuro, socio economic as well as other forms of diversity. The lack of diversity is further emphasised by the British Computer Society (BCS) analysis of the Information Technology (IT) workforce:[29]

- 17% female
- 17% non-white
- 21% over 50
- 8% disabled

[29] *British Computer Society (BCS) (2017) Diversity in IT 2017: shaping our future together. available at: https://www.bcs.org/upload/pdf/diversity-report-2017.pdf [accessed 28/03/19].*

Research by Ecorys[30] on behalf of DCMS draws attention to a number of market failures and barriers, including a lack of public knowledge of career prospects in the digital sector. Most notably there are obstacles for women with comparatively low numbers on higher education courses in computer related subjects, and within the industry as a whole, compared to their male counterparts.

There is also a perception problem surrounding the cyber security sector,[31] particularly with young women.[32] A study conducted by Arlington Research and Kaspersky Lab[33] found that the association of the industry with common terms such as 'hacker' were viewed negatively by young women. This is further emphasised by a survey which showed that 33% of young women thought that cyber security professionals were 'geeks', and a quarter saw them as 'nerds'. This was thought to be a contributing factor to the 78% who disregarded a career in cyber security. It is, therefore, difficult to attract women into the sector as career choices are often made before the age of 16. Women are one of the target groups for the CSIIF pilot.

In addition to the above barriers to entry there are also a range of social, institutional and personal barriers to the advancement of women who do choose a career in cyber security. There is criticism of the 'hacker culture' within the industry which perpetuates long hours, late nights and behaviours which can isolate women.[34] These obstacles can be difficult to overcome as professional women must balance home and career life much more than their male counterparts, leading to a perception that women lack strong career devotion.[35] This suggests that in addition to encouraging diverse candidates into the sector, more could be done to support their retention.

Neurodiverse individuals are another group targeted by the pilot. The Information Assurance Advisory Council (IAAC) has published a guide for employers which maps the typical strengths of neurodiverse individuals to the skills needed by cyber security analysts wishing to understand an innovative cyber attack. These include attention to detail, methodological approach, good memory for factual information, strong problem solving skills, strong numerical skills, different ways of thinking (or neurodiverse), specialist knowledge and skills, pattern recognition, reliable and resourceful.[36]

Although neurodiverse individuals often excel in schools and tertiary education, they are often faced with interpersonal challenges. Traditional recruitment and interview processes can create a barrier to neurodiverse people gaining meaningful employment.[37] According to the National Autistic Society, just 16% of autistic adults are in full-time paid employment, a statistic that has not

---

[30] *Ecorys (2016) Digital Skills for the UK Economyhttps://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492889/DCMSDigitalSkillsReportJan2016.pdf [accessed 08/05/19].*

[31] *Dallaway, E. (2017) closing the gender gap in cyber security, united kingdom: crest [online] available at: https://www.crest-approved.org/wp-content/uploads/CREST-Closing-the-Gender-Gap-in-Cyber-Security.pdf [accessed 03/06/2019].*

[32] *Centre for Strategy and Evaluation Services (2018) Identifying the Role of Further and Higher Education in Cyber Security Skills Development, United Kingdom: Department for Digital, Culture, Media and Sport. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/767425/The_role_of_FE_and_HE_in_cyber_security_skills_development.pdf [accessed 08/05/19].*

[33] *Kaspersky Lab (2017) Beyond 11%: A study into why women are not entering cybersecurity [online] Available at:* https://d1srlirzdlmpew.cloudfront.net/wp-content/uploads/sites/86/2017/11/03114046/Beyond-11-percent-Futureproofing-Report-EN-FINAL.pdf *[Accessed 15/02/2019].*

[34] *C.A. Heaton and E. McWhinney, "Women in Management: The Case of MBA Graduates," Women in Management Rev., vol. 14, no. 4, 1999, pp. 136–145.*

[35] *Women in cybersecurity: A study of career advancement: [online] Available at: file:///C:/Users/dsr1/Downloads/IEEE20IT20Professional.pdf [Accessed 15/02/2019]*

[36] *Information Assurance Advisory Council (IAAC) (2017) Autism and careers in cyber security: A short guide for employers, United Kingdom: Information Assurance Advisory Council (IAAC). available at: https://www.iaac.org.uk/wp-content/uploads/2017/07/Autism-and-careers-in-cyber-security-FINAL.pdf. [accessed 03/06/2019].*

[37] *Partridge, R. (2018) Tapping into neurodiversity for new cyber security skills, Available at: http://www.engineeringnews.co.za/article/tapping-into-neurodiversity-for-new-cyber-security-skills-2018-06-18/rep_id:4136 [Accessed: 20th February 2019].*

changed in almost a decade. Furthermore, just 32% of autistic adults are in any kind of paid work despite 77% of unemployed autistic adults stating that they want to work.[38]

2.5 Summary

Research indicates that more than half of all UK businesses have a basic cyber security skills gap and that this affects the majority of sectors.[39] There are insufficient skilled cyber security professionals to fill these gaps. There is also a lack of diversity in the sector[40] and a number of barriers to entry including a lack of awareness of career opportunities[41] and negative perceptions of the industry.[42] For women there are also barriers in terms of the proportion of women studying related subjects and subsequently entering the industry.[43] While for neurodiverse people traditional recruitment practices can be a barrier to employment.[44] This limits the flow of talent into the UK cyber security profession and confirms the need for government intervention, to boost the volume and diversity of people transitioning into entry-level cyber security jobs.

CSIIF has been designed to create more entry-level skilled people coming from a range of diverse backgrounds and therefore has the potential to contribute to the current government strategies[45] for cyber security skills. To be effective it needs to bring people into long term cyber security employment who wouldn't have otherwise been able to engage in the sector and do so in a cost-effective manner.

---

[38] *The National Autistic Society (2017) The autism employment gap - too much information in the workspace: The National Autistic Society. available at: file:///C:/Users/jrw3/Downloads/TMI%20Employment%20Report%2024pp%20WEB%20(1).pdf. [accessed 03/06/2019].*

[39] *Ipsos Mori (2018) Understanding the UK Cyber Security Skills Labour Market. [online]. available at: https://www.ipsos.com/sites/default/files/ct/publication/documents/2019-01/understanding_the_uk_cyber_security_skills_labour_market.pdf [accessed 08/05/19].*

[40] *British Computer Society (BCS) (2017) Diversity in IT 2017: shaping our future together. available at: https://www.bcs.org/upload/pdf/diversity-report-2017.pdf [accessed 28/03/19].*

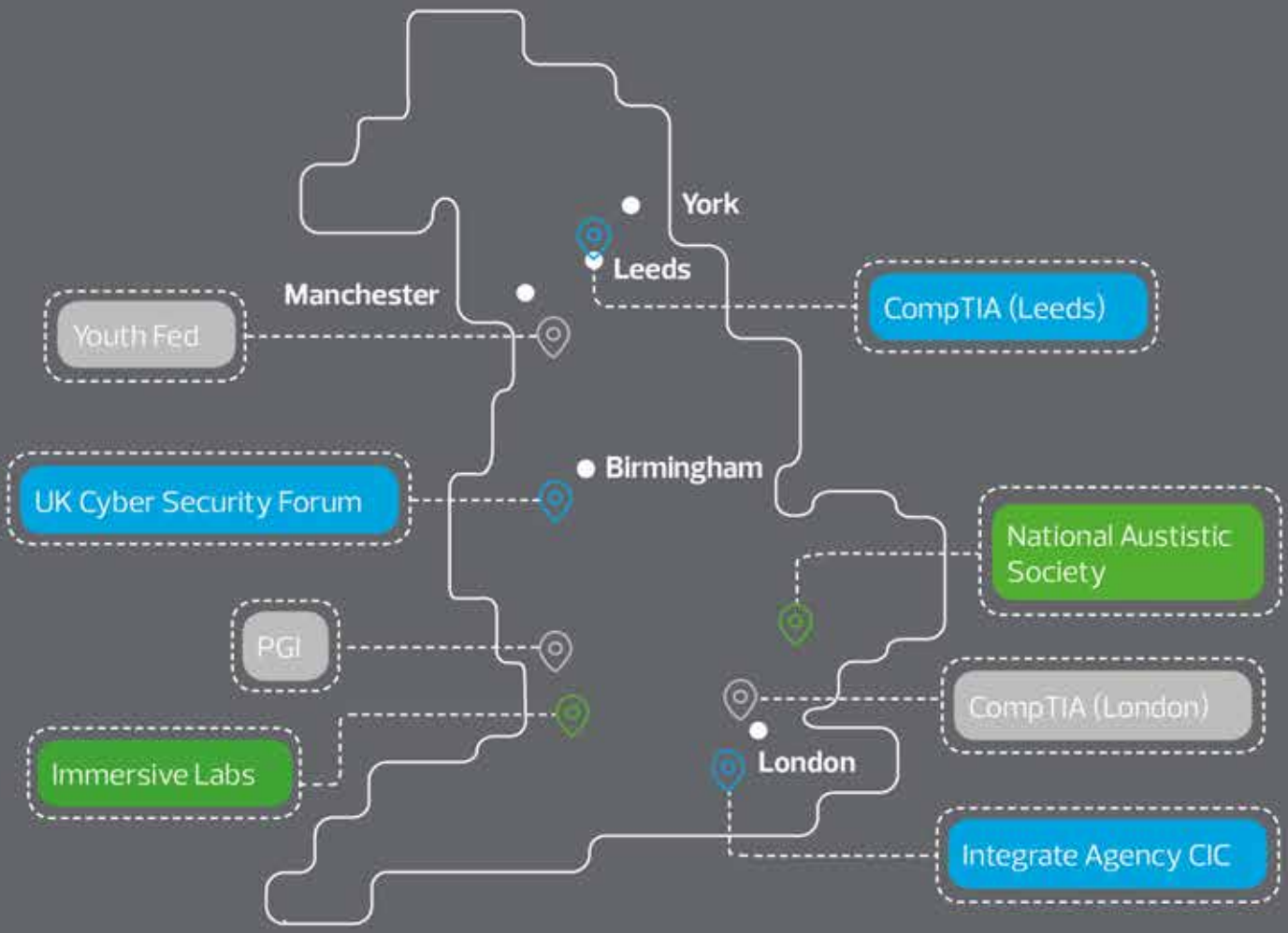
[41] *Ecorys (2016) Digital Skills for the UK Economy. [online]. available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492889/DCMSDigitalSkillsReportJan2016.pdf [accessed 08/05/19].*

[42] *Dallaway, E. (2017) closing the gender gap in cyber security, united kingdom: crest [online] available at: https://www.crest-approved.org/wp-content/uploads/CREST-Closing-the-Gender-Gap-in-Cyber-Security.pdf [accessed 03/06/2019]; Centre for Strategy and Evaluation Services (2018) Identifying the Role of Further and Higher Education in Cyber Security Skills Development, United Kingdom: Department for Digital, Culture, Media and Sport; Kaspersky Lab (2017) Beyond 11%: A study into why women are not entering cybersecurity [online] Available at: https://d1srlirzdlmpew.cloudfront.net/wp-content/uploads/sites/86/2017/11/03114046/Beyond-11-percent-Futureproofing-Report-EN-FINAL.pdf [Accessed 15/02/2019].*

[43] *Ecorys (2016) Digital Skills for the UK Economy. [online]. available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492889/DCMSDigitalSkillsReportJan2016.pdf [accessed 08/05/19].*

[44] *Partridge, R. (2018) Tapping into neurodiversity for new cyber security skills, Available at: http://www.engineeringnews.co.za/article/tapping-into-neurodiversity-for-new-cyber-security-skills-2018-06-18/rep_id:4136 [Accessed: 20th February 2019].*

[45] *HM Government (2016) National Cyber Security Strategy (2016-2021). [online]. available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf [accessed 08/05/19]; HM Government (2018) initial national cyber security skills strategy. available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/767515/Cyber_security_skills_strategy_211218.pdf [accessed 01/04/19]; HM Government (2017) UK digital strategy. [online] available at: https://www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy [accessed 08/05/19].*


York
Leeds
Manchester
Youth Fed
CompTIA (Leeds)
Birmingham
UK Cyber Security Forum
National Austistic Society
PGI
CompTIA (London)
London
Immersive Labs
Integrate Agency CIC

3. INTERVENTION

3.1 Overview

This section provides a summary of the CSIIF initiative and how it is being implemented. It is structured under the following sub headings:

- Aims and objectives of the pilot – *outlining the CSIIF aims and objectives*
- Design of the pilot – *describing how the pilot was developed*
- Implementation of the pilot – *summarising how the pilot is being delivered by DCMS and the CSIIF funded projects*
- Monitoring and reporting – *setting out the monitoring and reporting requirements for projects*
- Summary – *presenting findings in relation to the above*

3.2 Aims and objectives of the pilot

CSIIF aims to develop the pipeline of UK cyber security talent by training individuals, not currently engaged in the sector, for entry-level cyber security roles. It also aims to boost the diversity of the sector, particularly in relation to women and neurodiverse candidates.

It does this by providing grant funding for organisations to develop, scale up, or refocus their cyber security training projects to help equip individuals for entry-level cyber security roles within 6 months. There is also a focus on developing sustainable training provision to enhance vocational cyber security training provision across the UK.

3.3 Design of the pilot

In 2017 DCMS undertook a stakeholder engagement exercise across the UK. The design and review of this process was carried out by an independent contractor. As a result of this exercise DCMS concluded that:

- a range of cyber security retraining activity is already taking place
- providing initial seed-funding to support pilots and proof of principle projects would be a more sustainable method of government intervention to stimulate a cyber retraining system in the immediate term

DCMS ran a competition between February and March 2018 inviting organisations to submit proposals for projects that aim to get non-cyber security professionals into entry-level cyber security roles within 6 months. This included a small communications campaign using social media and industry communications forums to publicise the opportunity. DCMS received 25 applications from 18 different organisations.[46]

[46] *EACH ORGANISATION WAS ALLOWED TO SUBMIT UP TO THREE APPLICATIONS TO THE FUND.*

The applications were reviewed, challenged and assessed by a cross departmental group against a detailed framework, which included:

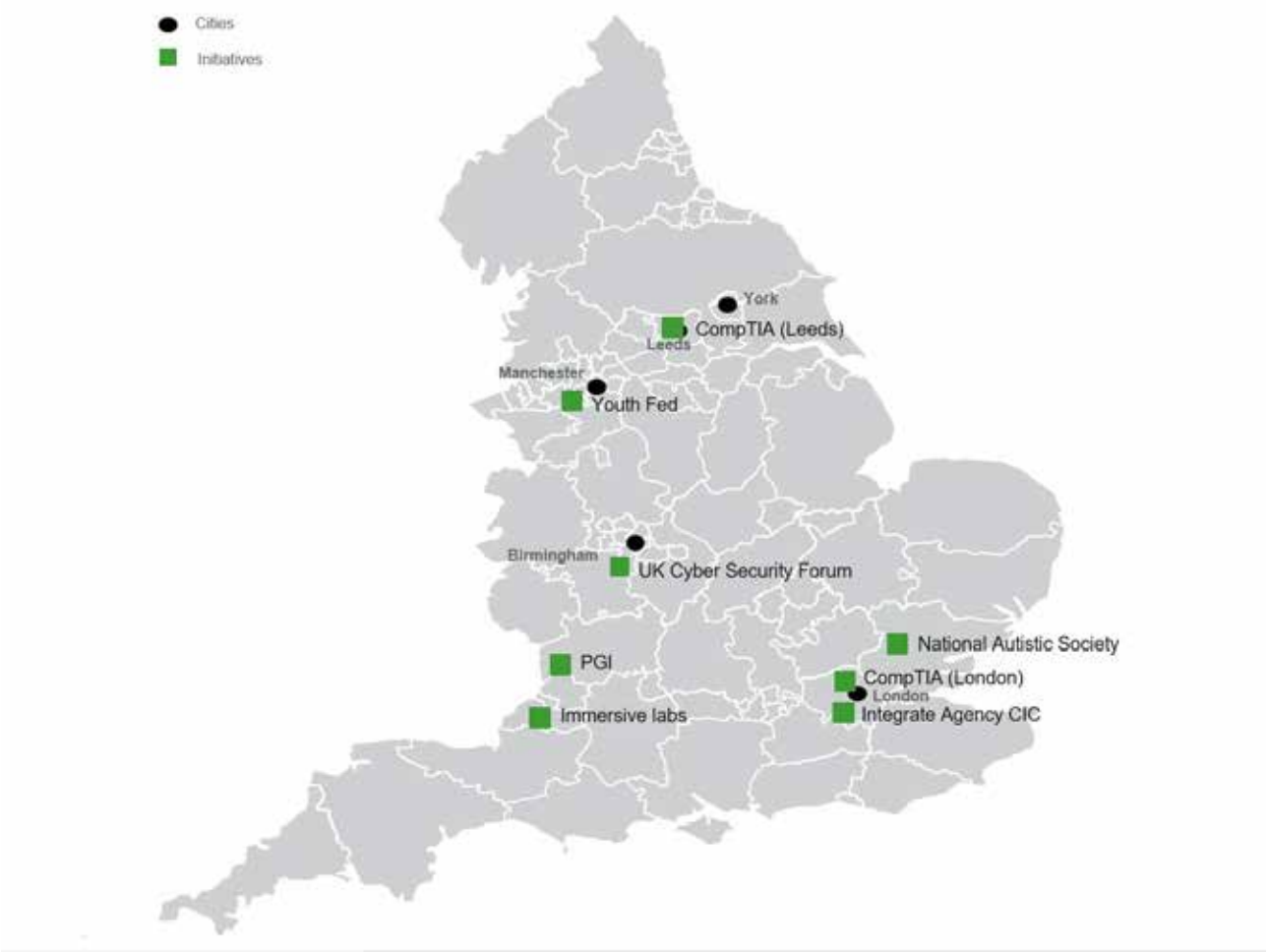
- the organisation's experience
- ability to directly impact the cyber skills shortage
- fit of the initiative's aims, outcomes, beneficiaries and outputs with the CSIIF objective
- fit with funding criteria
- additionality of the project
- relevant and realistic deliverables, milestones and timeframes
- suitability of project team
- risk management and mitigation
- wider social and economic benefits
- employment outcomes
- equal opportunities and diversity
- ability to evidence outputs and deliverables, monitor appropriate stakeholder data and capture lessons learnt
- project finances including other sources of funding, financial management, project budget and payment profile

Seven applications were successful and received CSIIF grants ranging between £20,000 and £70,000 each, with providers contributing additional cash or in-kind contributions (match funding) of at least half of the total project cost. Providers welcomed the flexibility of the fund, in terms of allowing providers to propose their own payment schedule and providing advance funding where it was needed.

While the number of successful projects exceeded DCMS expectations, one sector representative felt that notifying a broader range of providers further in advance of the competition could help to encourage applications from a wider group of providers, potentially increasing the diversity and number of proposals.

Figure 3.1 overleaf maps the location of the 7 projects across England. It shows a good balance between provision in the North and South of England. A number of projects also offer training online for increased accessibility. Given the relatively small number of projects involved in the pilot, it is unrealistic to expect to achieve a physical presence in all parts of the country. However, as the fund expands, the selection criteria should consider areas of the country where there are gaps in provision. There may also be an opportunity to work with local Digital Skills Partnerships to make sure that provision supports the most deprived areas.

Figure 3.1: Location of CSIIF providers



SOURCE: RSM ANALYSIS

NOTES:

COMPTIA - CYBER READY HAS AN ONLINE PLATFORM AND HOSTS FACE-TO-FACE WORKSHOPS AT SITES IN LEEDS AND LONDON

IMMERSIVE LABS - NEURODIVERGENT DIGITAL CYBER ACADEMY PROVIDES TRAINING VIA AN ONLINE PLATFORM

3.4 Implementation of the pilot

The pilot projects cover a broad range of target groups and are testing proof of principle of a variety of training approaches to address the market failures identified in Section 2. These are summarised in Table 3.1 and described in detail in Appendix A.

Table 3.1: Successful CSIIF projects

Org.	Initiative	Target group	Summary
CompTIA	Cyber Ready	• Neurodiverse individuals • Women • Black, Asian, and minority ethnic (BAME) • Economically deprived	A 6 month project for candidates from a diverse range of backgrounds to upskill around existing work and caring requirements to become ready for a career in cyber security.
Immersive Labs	The Neurodivergent Digital Cyber Academy	• Neurodiverse individuals	The Academy is designed to help neurodiverse candidates develop their cyber security skills through hands-on practical challenges via an online platform.
National Autistic Society (NAS)	NAS Enterprise Cyber Security Programme	• Neurodiverse individuals (focusing on autistic people)	A cyber security apprenticeship scheme specifically for autistic people. The project will support candidates through cyber security training and preparation for employment.
PGI Cyber Academy	Lifelong learning career paths for Women Cyber Security Professionals	• Women career transitioners	A professional conversion project for women transitioning into entry-level cyber security jobs from both technical and non-technical disciplines.
The Integrate Agency CIC	Cyber Safe Lambeth	• Lone parents in Brixton	A Brixton-based project which will provide lone parents in Lambeth with practical cyber security training, with the aim of creating a thriving community of cyber security expertise in Lambeth.
UK Cyber Security Forum CIC	Community Cyber Security Centre	• Neurodiverse individuals	A Community Cyber Security Centre in Worcester, with the aim of training neurodiverse individuals in cyber security, while developing services to protect the internet access of vulnerable members of society.
Youth Fed	Cyber Threat Hub Academy	• Young adults	A Cyber Security Operations Centre (SOC) based in Salford, which aims to replicate real-world work experience for young adults interested in a career in cyber security.

SOURCE: RSM ANALYSIS

Partnerships have developed between a number of the funded projects creating synergies. For example, UK Cyber Security Forum - Community Cyber Security Centre provides employability training and support for neurodiverse individuals who developed their cyber security skills through the Immersive Labs - Neurodivergent Digital Cyber Academy. The NAS - Enterprise Cyber Security Programme is also using Immersive Labs - Neurodivergent Digital Cyber Academy to help identify suitable apprentices.

In addition to the barriers identified in Section 2 of this report CSIIF providers identified a number of barriers affecting the demand for their projects from potential candidates. These are summarised in Table 3.2, along with the support they are providing to address these barriers.

Table 3.2: Barriers affecting demand for CSIIF funded training provision

Barrier	Affected group	Support provided via CSIIF projects to overcome these barriers
Lack of information about the range of opportunities	All	Raising awareness about opportunities in the sector Guest speakers from industry
Ability to engage in traditional recruitment processes	Neurodiverse individuals	Employability support (CV development and interview techniques) Introducing candidates to partners and employers Training in a group setting with peers Trainers who specialise in special educational needs
Lack of confidence/ imposter syndrome	Women and returners	Employability support (CV development and interview techniques) Peer support Closed communication groups for candidates to share problems and best practice Providing experience in a live environment that replicates real work conditions Introducing candidates to employers
Employment being sufficiently lucrative	Lone parents	Raising awareness about opportunities in the sector Employability support (CV development and interview techniques) Awarding industrial certifications which employers' value
Flexibility balanced with care needs	Lone parents	Flexibility in course delivery

SOURCE: CSIIF PROVIDER CONSULTATIONS

The consultations with CSIIF providers identified how the pilot funding has allowed them to offer new benefits to candidates in the form of:

- accessibility - *providing increased access to hardware, flexible learning (online, anywhere, anytime) and offering a range of times, venues and days for workshops*
- breadth of support - *including structured learning plans and targets and partnerships with other projects that provide complementary services (for example, technical training interventions working with employability projects)*

3.5 Monitoring and reporting

A DCMS Policy Adviser is responsible for managing the pilot and monitoring the development of CSIIF projects, with oversight from the Policy Lead and Head of Cyber Security Skills and Professionalisation. To provide proof-of-principle of the pilot, providers are required to submit formal reports to DCMS on activities, progress towards milestones and expenditure on a quarterly basis, as well as informal reporting to capture lessons learned from the pilot. Our consultations found that the CSIIF providers do not consider the reporting requirements to be onerous and welcomed the flexibility to include additional information and unanticipated benefits. It is our assessment that further information could be collected from providers to assist in the evaluation of the funding.

For example, the following logic model has been developed by RSM as part of this evaluation (Table 3.3). It sets out the indicators at output, outcome and impact level that can be used to measure the performance of the pilot. Agreement of such a logic model, allows the agreed indicators to be included into letters of offer/ funding agreements with providers and monitoring to take place against these. This model should be used to measure the impact of the pilot in the future and tailored accordingly for future funding opportunities.

Table 3.3: CSIIF logic model

Inputs	Activities	Outputs	Outcomes	Impacts
• DCMS funding • Match funding • DCMS staff time – for management and administration	• Small communications campaign • Setting up processes to administer the grant • Grant management and administration • Marketing by CSIIF providers • Training provision • Events • Employer engagement	• Total no. of applications to the pilot by gender, neurodiversity and ethnicity • Total no. of candidates by gender, neurodiversity and ethnicity • No. of candidates who have completed their training by gender, neurodiversity and ethnicity • No. of employers engaged and involved in supporting the project	• Number of people (from each target beneficiary group) with basic cyber security skills/ qualifications • Number of people (from each target beneficiary group) getting jobs in cyber security • Length of time in cyber security role (eg over one year) by target beneficiary group	• Increase in the number of entry-level cyber security professionals in the UK • Increase in the diversity of entry-level cyber security professionals in the UK • Increase in the number of vocational cyber security training providers

SOURCE: RSM ANALYSIS

The DCMS policy team has verified 87% of CSIIF funding to date. This has not resulted in any verification adjustments. Note: verification of expenditure focuses on CSIIF funding only, it does not include match funded expenditure. Projects are also subject to random audits from the DCMS finance and grants team.

3.6 Summary

CSIIF has been successfully implemented and is funding 7 projects. These projects are geographically dispersed, cover a suitably broad range of target groups and are implementing a variety of training methods to test proof of principle. The provider consultations found evidence of projects working together to create synergies.

The number of provider applications received exceeded DCMS expectations. However, one sector representative felt that advertising the opportunity further in advance and with a wider group of providers would encourage more diverse proposals (Recommendation 2).

While DCMS has verified 87% of CSIIF spend to date, no verification of match funding has been undertaken. We suggest that DCMS introduce this requirement in the future (Recommendation 3).

The monitoring of the performance of the funded projects could be strengthened by requiring any future providers to provide further information on the range of outputs and impacts as set out in the logic model developed by RSM for CSIIF. This provides DCMS the opportunity to get a more comprehensive view of the development and ultimately performance of CSIIF.


478
people
taking part
23.8%
are female
55.3%
have a
neurodiverse condition
10.1%
are from an ethnic
minoirty background
Based on information from 4 of the 7 providers, 3 providers did not record information on the ethnic background of their candidates

4. PERFORMANCE

4.1 Overview

This section assesses the performance of the CSIIF pilot. It includes the following sub headings:

- Expenditure – *analysis of the draw down and match funding*
- Effectiveness[47] – *summary of progress towards the target outputs of the pilot and the outcomes achieved to date*
- Additionality – *assessment of the extent to which the outputs and outcomes achieved are because of CSIIF*
- Summary – *presenting findings in relation to the above*

4.2 Expenditure

In line with rules around disclosure of funding amounts under the National Cyber Security Programme some financial information, including assessment of value for money, is not included in this published version.

The 7 projects have drawn down the bulk of their grant allocation (93.2% of total grant award as of May 2019).[48] There have been significant delays to the PGI Cyber Academy project, however as of May 2019, this training is still expected to take place.

It was a condition of CSIIF funding that providers secure match funding for at least half of the total costs of the project. Providers felt that the reputational benefits of being associated with a DCMS initiative helped them to leverage additional funding. The total amount of match funding achieved is greater than the total CSIIF grant award. **It should be noted that this is based on data reported via the CSIIF provider consultations. It has not been verified by RSM or DCMS.**

The creation of 7 new training pathways and the fact that the pilot is on track to drawdown the majority of grant funding awarded, suggests that the fund has been successful in its aim of stimulating the market to build an immediate route into the cyber security talent pipeline.

4.3 Effectiveness

4.3.1 Outputs

There are 478 people taking part in the pilot (138.2% of target), of whom:

- Almost a quarter are women (23.8%)
- Over half have a neurodiverse condition (55.3%)
- A tenth are from ethnic minority backgrounds (10.1%)[49]

---

[47] *MEASURED AS THE EXTENT TO WHICH THE PILOT HAS MET ITS OBJECTIVES (SOURCE: HM TREASURY (2011). THE MAGENTA BOOK: GUIDANCE FOR EVALUATION [ONLINE] AVAILABLE AT: HTTPS://ASSETS.PUBLISHING.SERVICE.GOV.UK/GOVERNMENT/UPLOADS/SYSTEM/UPLOADS/ATTACHMENT_DATA/FILE/220542/MAGENTA_BOOK_COMBINED.PDF [ACCESSED 22/03/2019].)*

[48] *IN LINE WITH RULES AROUND DISCLOSURE OF FUNDING AMOUNTS UNDER THE NATIONAL CYBER SECURITY PROGRAMME SOME FINANCIAL INFORMATION, INCLUDING ASSESSMENT OF VALUE FOR MONEY, IS NOT INCLUDED IN THIS PUBLISHED VERSION.*

[49] *THIS IS BASED ON INFORMATION FROM 4 PROJECTS, THE REMAINING 3 DID NOT RECORD CANDIDATES' ETHNIC BACKGROUND*

The project has, therefore, been somewhat successful in encouraging diversity. The fund has achieved 89.8% of its target for the number of women trained (127). It should be noted, however, that not all candidates chose to provide their gender and the training by PGI, which focuses on women transitioners, is still expected to take place.

The number of neurodiverse candidates (264) trained has substantially exceeded its target (of 157, achieving 168.2% of target). No targets were set in relation to the ethnic diversity of candidates, but 10.1% of candidates is in line with the Office for National Statistics (ONS) data on ethnic diversity in England and Wales.[50]

Two projects have yet to complete their training (as of May 2019), which will limit the potential impact of the training to date.

Four projects revised their original targets in agreement with DCMS, due to difficulty engaging with their target groups. In some cases, the revisions were considerable. Table 4.1 summarises the performance of each of the 7 projects against their revised targets for the number of candidates taking part. Assessment of the performance of each project in relation to the number of female, neurodiverse and BAME candidates is based on the proportion of all candidates taking part.

[50] *86% of the population gave their ethnic group as 'white' in the 2011 Census (source: ONS (2012) Ethnicity and National Identity in England and Wales: 2011. [online]. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/culturalidentity/ethnicity/articles/ethnicityandnationalidentityinenglandandwales/2012-12-11 [accessed: 03/04/2019].)*

Table 4.1: Performance as of May 2019

Organisation	No. of applicants	Candidates taking part on initiative		Female candidates taking part		Neurodiverse candidates taking part		BAME candidates taking part		Candidates completed training		candidates placed into employment		
		n	% of target	n	% of total	n	% of total	n	% of total	n	% of total	n	% of total	% who have completed training
CompTIA	89	30	100.0%	5	17.0%	4	13.0%	10	33.0%	27	90.0%	12	40.0%	44.4%
Immersive Labs	138	193	241.3%	N/A	N/A	193	100.0%	N/A	N/A	N/A	N/A	N/A	N/A	0.0%
National Autistic Society	12	6	50.0%	2	25.0%	6	100.0%	N/A	N/A	0	0.0%	0	0.0%	0.0%
PGI Cyber Academy	360	0	0.0%	0	0.0%	0	0.0%	0	0.0%	0	0.0%	0	0.0%	0.0%
The Integrate Agency CIC	72	25	52.1%	22	87.0%	0	0.0%	20	78.0%	25	100.0%	12	48.0%	48.0%
UK Cyber Security Forum CIC	20	37	1850.0%	5	14.0%	37	100.0%	N/A	N/A	23	62.2%	20	54.1%	87.0%
Youth Fed	187	187	124.7%	80	43.0%	24	13.0%	19	10.0%	187	100.0%	0	0%	N/A
Total	**878**	**478**	**138.2%**	**114**	**23.8%**	**264**	**55.3%**	**48**	**10.1%**	**262**	**54.8%**	**44**	**9.2%**	**16.8%**

SOURCE: DCMS

NOTES:

PROJECTS DO NOT REPORT ON CANDIDATE DROPOUT RATES

CANDIDATES FROM IMMERSIVE LABS DO NOT TECHNICALLY 'COMPLETE' THE INITIATIVE. THESE 193 CANDIDATES HAVE COMPLETED AT TOTAL OF 8,389 INDIVIDUAL LABS, EQUATING TO ROUGHLY 1,900 HOURS SPENT ON THE TRAINING PLATFORM

DUE TO PROJECT DELAYS NO TRAINING HAS TAKEN PLACE UNDER THE PGI CYBER ACADEMY AS OF 31 MAY 2019. THIS ACTIVITY IS STILL EXPECTED TO TAKE PLACE AT A LATER DATE

Analysis of project monitoring information (Table 4.1) shows that, for most projects (4 out of 7), the overall number of candidates taking part in their training is in line with or exceeding the targets agreed with DCMS. However, a number of providers reported difficulty attracting candidates from their target groups, particularly neurodiverse individuals who are typically less well networked and hard to reach. Providers have found, therefore, that it is taking longer than anticipated for the employability outcomes to materialise for this group. These providers stated that the engagement and education of employers has been slower than expected, resulting in a longer lead in time for their projects (NAS- Enterprise Cyber Security Programme, UK Cyber Security Forum CIC- Community Cyber Security Centre and Youth Fed- Cyber Threat Hub Academy). The majority of projects still expect most candidates to transition into cyber employment within 3 to 6 months of completion of the project.

Those who were successfully engaging with target beneficiaries noted that partnerships with other projects and building their reputation with their target groups and the relevant referral agencies for those groups contributed to their success. Projects that targeted women and lone parents said that word of mouth and social media had been particularly effective in attracting potential candidates from these groups.

One provider, who was targeting new entrants to the sector, was surprised by the number of people with software development experience and qualifications that it attracted (approximately half of all candidates taking part).

4.3.2 Outcomes

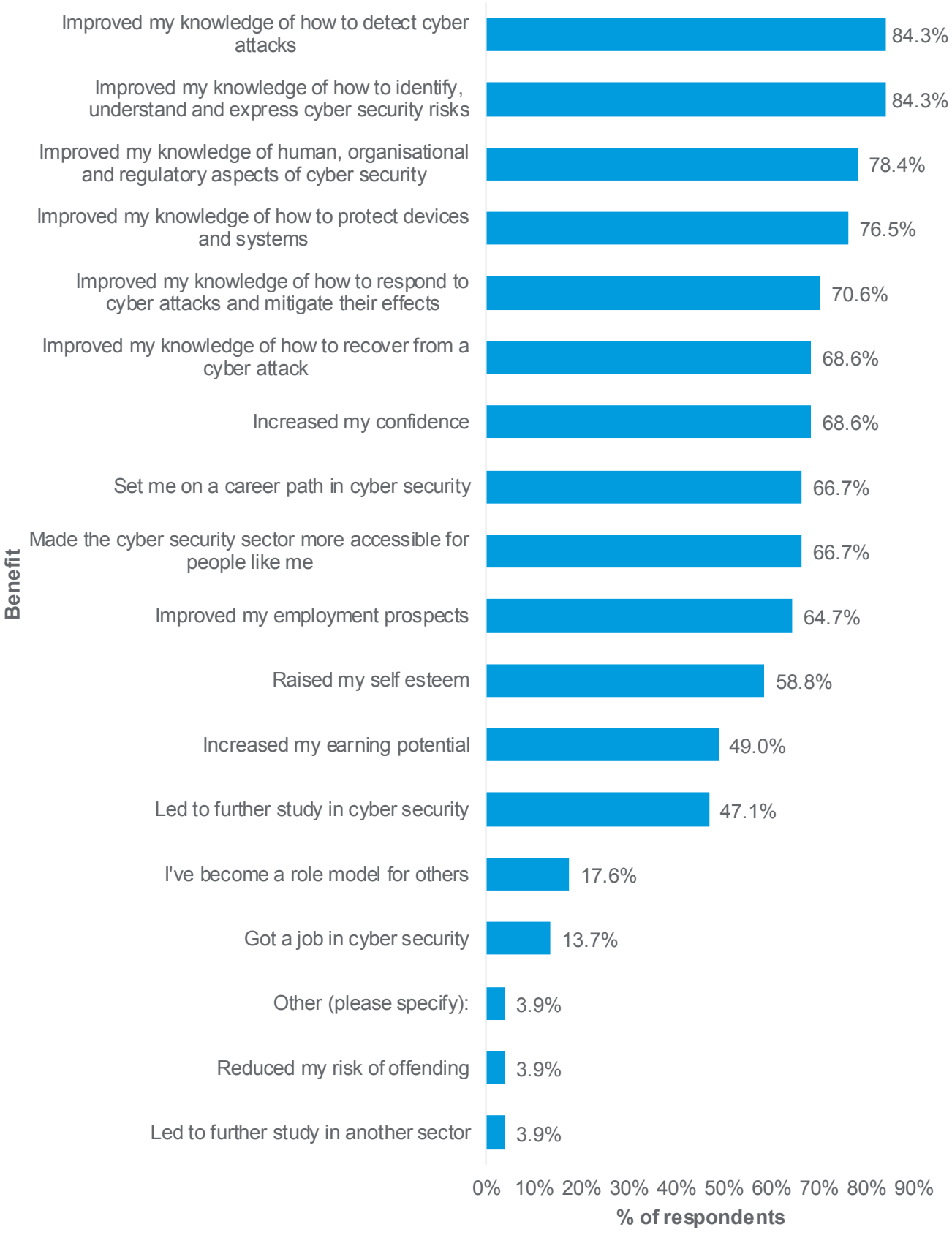
The aim of the pilot is to retrain candidates for employment in entry-level cyber security roles within 6 months. While the pilot has exceeded its target for the number of candidates taking part (478), 2 projects have yet to complete their training and only 44 candidates (9.2% of those taking part) have been placed into employment to date. This is equivalent to 16.8% of candidates who have completed their training. It should also be noted that these roles vary from internships to work placements to paid employment. DCMS should establish a clear definition of the type of employment it intends candidates to be engaged in within 6 months of completing their project (Recommendation 4).

Youth Fed is different from the other CSIIF projects in that it is aimed at young people. As such its candidates are not expected to transition into employment in the short term. Instead it aims to encourage more young people to pursue a career in cyber security. Follow up research on the training and employment destinations of Youth Fed candidates is required to determine whether it has been effective in this respect and the extent to which it has acted as a feeder project for other cyber security training initiatives.

Figure 4.1 overleaf illustrates the benefits reported by respondents of the beneficiary survey. It should be noted that the majority of survey respondents (74.1%) were still completing their CSIIF course, which will limit the effect it has had on them to date. The benefits most commonly reported by respondents were that they improved their knowledge of:

- how to detect cyber attacks (84.3%)
- how to identify, understand and express cyber security risks (84.3%)
- the human, organisational and regulatory aspects of cyber security (78.4%)
- how to protect devices and systems (76.5%)

Figure 4.1: Benefits of CSIIF training – Beneficiary survey



BASE: 51

Interestingly, given the target groups, over half of respondents reported that participation had raised their self esteem (58.8%), which is very positive, but only 17.6% felt that they had become a role model for others wishing to enter the sector. When these responses are considered in relation to the target groups it shows that:

- 72.7% of female respondents reported an increase in confidence, 63.6% reported raised self esteem, 9.1% had become a role model, and 72.7% felt the project had made cyber security more accessible for people like them
- 66.7% of neurodiverse respondents reported an increase in confidence, 76.2% reported raised self esteem, 28.6% had become a role model, and 61.9% felt the project had made cyber security more accessible for people like them
- 68.4% of respondents from ethnic minority backgrounds reported an increase in confidence, 68.4% reported raised self esteem, 15.8% had become a role model, and 78.9% felt the project had made cyber security more accessible for people like them

This suggests that DCMS, the NCSC and CSIIF providers, could do more to reinforce the idea that the people participating in these projects are leading the diversification of the cyber security industry. For example, by conducting site visits and promoting success stories (Recommendation 7). This could also help to address the retention issues identified in the literature review.[51]

Only 13.7% of respondents said that they had got a job in cyber security as a result of taking part in the CSIIF pilot, however, when this response is considered in relation to the 14 respondents who had completed their course it becomes (35.7%), with 64.3% of these respondents saying that it had set them on a career path in cyber security.

RSM followed up with survey respondents who had given consent to be contacted to understand how, in their opinion, the following similar responses differed: 'set me on a career path in cyber security', 'improved my employment prospects' and 'got a job in cyber security'. Their feedback indicates that respondents consider 'employment prospects' generally, which may have been good before taking part in the course, but not on a 'cyber security career path'. The difference between these responses and 'got a job' was securing a job.

Youth Fed, was unable to distribute the survey link as it does not hold contact details for its candidates. It was able, however, to share feedback it had collected from 60 candidates (see Table 4.2). This shows that the project has successfully met the expectations of all bar one candidate and that the majority of candidates (80.0%) would now consider a career in cyber security.

[51] *C.A. Heaton and E. McWhinney, "Women in Management: The Case of MBA Graduates," Women in Management Rev., vol. 14, no. 4, 1999, pp. 136–145. [online]. available at: https://www.emeraldinsight.com/doi/abs/10.1108/09649429910274815 [accessed 03/06/2019]; Women in cybersecurity: A study of career advancement: [online] Available at: file:///C:/Users/dsr1/Downloads/IEEE20IT20Professional.pdf [Accessed 15/02/2019]*

Table 4.2: Candidate feedback provided by Youth Fed

	Yes	No	Don't know
Has your SOC experience been what you expected?	59 (98.3%)	1 (1.7%)	-
Based upon todays experience and learning would you consider a career in cyber security	48 (80.0%)	2 (3.3%)	10 (16.7%)

SOURCE: YOUTH FED

CSIIF providers also noted the following additional outcomes of the pilot:

- guest speakers have helped to address one of the market failures identified in the literature by increasing candidates' awareness of cyber security and career opportunities in the sector
- a number of candidates will also have a more informed approach to job applications and interviews as a result of employability support, thus addressing a barrier identified in the literature review to the employment of neurodiverse people
- two individuals have been diverted from committing a cyber crime and are currently employed in cyber security roles with good links with the police

4.4 Additionality

Additionality is the extent to which something happened as the result of an intervention that would not have happened without the intervention.[52] Whist some of the outcomes listed in Section 4.3 could have been achieved without DCMS intervention, due to the range and complexity of barriers facing these groups and lack of alternative provision and/ or funding sources, it is unlikely they could have been delivered to the same scale or quality.

Most providers said their project would not have happened at all without CSIIF funding. Those that could have gone ahead with their initiative said that they would have had to do so on a much smaller budget. One of the providers, whose application for CSIIF funding was unsuccessful, said that CSIIF funding would have enabled them to deliver more activities. This organisation has still been able to run their initiative without the CSIIF, but on a smaller scale, delivering activities over the same time period but with fewer beneficiaries. This has resulted in a smaller impact compared with the impact of their proposed CSIIF project.

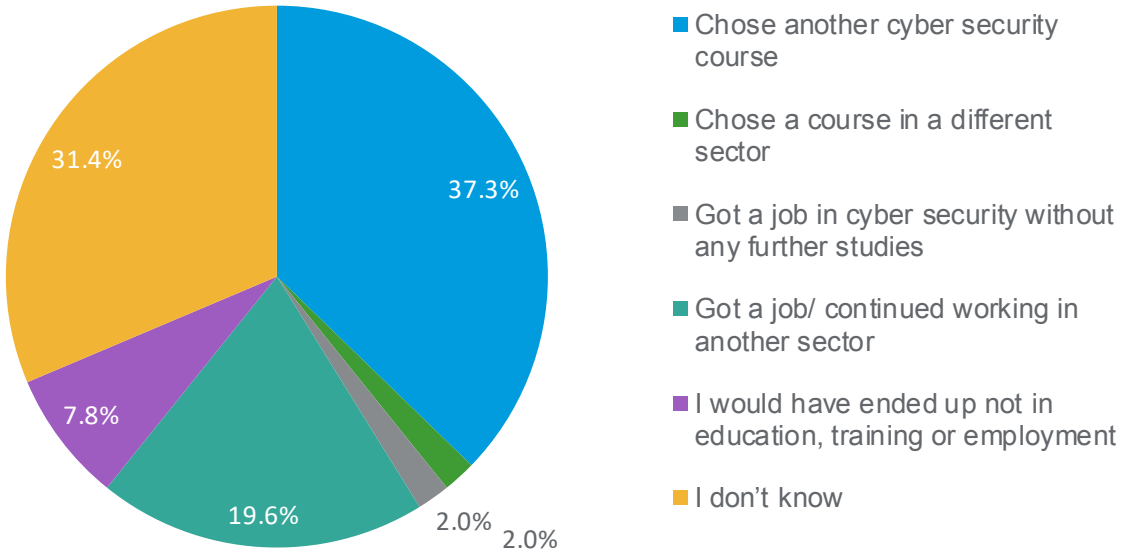
Providers also noted that DCMS sponsorship of their initiative had helped to leverage other funding and/ or in-kind support, including from private sector cyber security companies. This indicates employer buy-in for the pilot.

To understand what candidates would have done in the absence of CSIIF, the beneficiary survey asked respondents what they would have done had their application been declined (see Figure 4.2 overleaf). Over a third (37.3% of respondents) stated that they would have chosen another cyber security course while 2.0% thought they would have got a job in cyber security without any further study. Indicating that approximately 40% of respondents believe they would have engaged with the sector, in some form, without the pilot. A further 19.6% said that they would have got a job or

[52] *ENGLISH PARTNERSHIPS (2008) ADDITIONALITY GUIDE. [ONLINE]. AVAILABLE AT: HTTPS://ASSETS.PUBLISHING.SERVICE.GOV.UK/GOVERNMENT/UPLOADS/SYSTEM/UPLOADS/ATTACHMENT_DATA/FILE/191511/ADDITIONALITY_GUIDE_0.PDF [ACCESSED 28/03/19].*

continued working in another sector. 16 respondents (31.4%) did not know what they would have done without CSIIF.

Figure 4.2: What would you have done if your application had been declined? - Beneficiaries

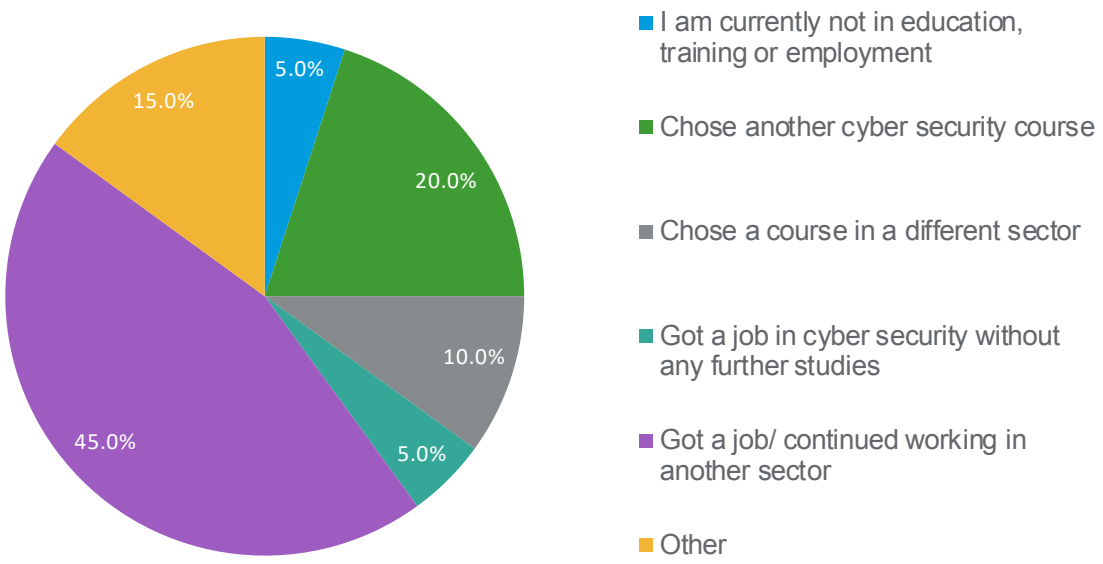


BASE: 51

To provide a comparison, we surveyed a control group of unsuccessful applicants to ask what they had done when their application was declined (see Figure 4.3 overleaf). Interestingly the proportion of respondents in the control group who said they chose another cyber security course was lower than the proportion of beneficiaries who said the same (20.0% compared to 37.3%), indicating that the number who were actually able to engage in another cyber security course could be lower than those who intended to do so. Similarly, the proportion of respondents in the control group who got a job or continued working in another sector (45.0%) was more than double the proportion of beneficiaries who said the same (19.6%). Other sectors that respondents went on to study or work in included:

- HM Forces
- IT (including hardware and software)
- IT support in the financial sector
- Retail

Figure 4.3: What did you do when your application was declined? – Control group



BASE: 20

The control group was also asked if they are currently employed in a cyber security role. Only 1 (5.6%) of the 18 respondents stated that they are currently working in the sector. The remaining 17 (94.4%) are not.

The bases for both the beneficiary survey and the control survey are low and, therefore, the following extrapolation needs to be treated with caution.

We can use the responses presented in Figures 4.2 and 4.3 to estimate the extent to which the cyber security outputs and outcomes presented in this section could have been achieved without the CSIIF pilot (see Table 4.3 overleaf). This results in an estimated additionality range of between 60% and 75%, which suggests that around 290 to 360 candidates would not have been engaged in cyber security training without the pilot and 26 to 33 candidates would not be employed in cyber security.[53] However, some of them would have engaged in other types of training and been employed in other sectors.

[53] *HOWEVER, CONSULTATION WITH THE 3 PROVIDERS THAT HAVE PLACED THE 44 CANDIDATES INTO EMPLOYMENT INDICATES THAT APPROXIMATELY 30% OF THESE CANDIDATES WERE ALREADY EMPLOYED IN A RANGE OF OTHER SECTORS BEFORE TAKING PART IN THEIR TRAINING. APPLYING THAT RATIO TO THE RANGE OF NET JOBS CREATED (26-33) RESULTS IN BETWEEN 8 AND 10 OF THE NET JOBS BEING TAKEN BY PEOPLE WHO TRANSITIONED FROM OTHER SECTORS.*

Table 4.3: Estimated additionality for the cyber security sector

	Beneficiaries	Control Group
Chose another cyber security course	37.3%	20.0%
Got a job in cyber security without any further studies	2.0%	5.0%
Total (%)	**39.3%**	**25.0%**
Estimated additionality for the cyber security sector (%)	**60.7%**	**75.0%**

NOTE: LEAKAGE[54] IS ASSUMED TO BE 0% AS THERE IS NO EVIDENCE OF CANDIDATES LEAVING THE UK

4.4.1 Sustainability

Sustainability of the CSIIF projects is important as this will contribute to the aim of developing the cyber security vocational training environment. It will also improve the additionality of the pilot if the provision is sustainable in the long term. CSIIF providers are at various stages in their sustainability plans. These include:

- developing social enterprise/ consultancy models and/ or bidding for public sector contracts (CompTIA, the Integrate Agency CIC and UK Cyber Security Forum CIC)
- exploring industry sponsorship (CompTIA, PGI Cyber Academy and Youth Fed)
- minimising their running costs by refocusing their online platform (Immersive labs) or using alternative funding and staffing models (Youth Fed)

[54] *LEAKAGE: THE PROPORTION OF OUTPUTS THAT BENEFIT THOSE OUTSIDE OF THE INTERVENTION'S TARGET AREA OR GROUP*

4.5 Summary

Almost 480 candidates have taken part in the pilot to date. This exceeds the overall target for the fund (by 38.2%). Good progress has been made towards the target for the number of female candidates (127) and the target for neurodiverse candidates (157) has been exceeded (achieving 89.8% and 168.2% of target respectively). The project has been successful in attracting more diverse candidates into the sector:

- 23.8% of candidates are female
- 55.3% of candidates have a neurodiverse condition
- 10.1% of candidates are from ethnic minority backgrounds[55]

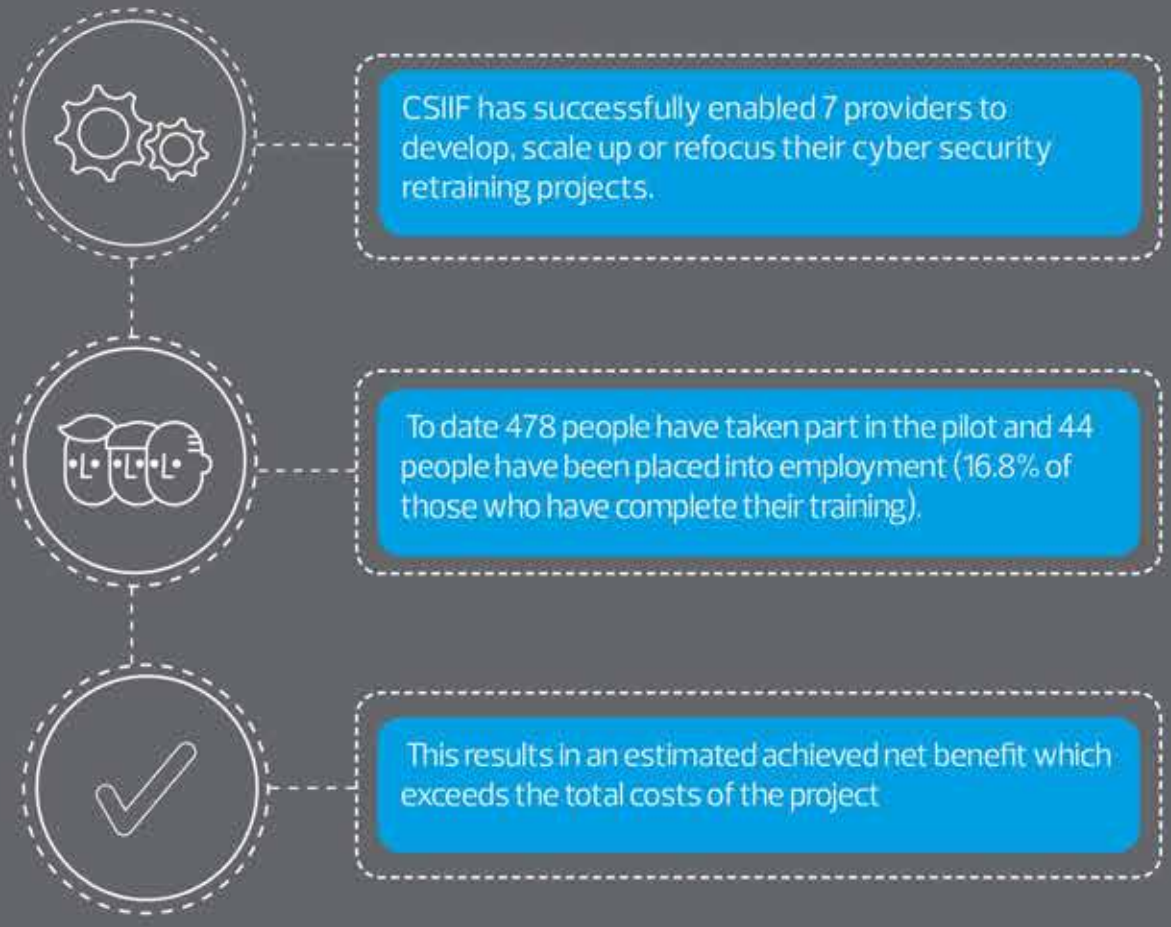
Providers indicate that the lead in time required for some projects was longer than expected. This should be factored into future funds to help set more realistic timeframes and targets (Recommendation 5).

44 candidates have been placed into employment to date. This is equivalent to 16.8% of those who had completed their training. While the majority of survey respondents (74.1%) were still completing their training, they were already able to identify a range of positive outcomes, including increased technical knowledge (over two thirds of respondents), increased confidence (68.6%) and self esteem (58.8%). However, the low number of candidates who viewed themselves as role models for others wishing to enter the sector (17.6%) suggests that DCMS, the NCSC and CSIIF providers could do more to celebrate the fact that these people are pioneers for diversity within the sector.

The ability of the pilot to attract match funding is also evidence of employer buy-in.

There is evidence that the providers would not have been able to deliver these projects at the same scale without CSIIF funding. The estimated additionality range for the pilot is between 60% and 75%, which suggests that approximately 290 to 360 candidates would not have been engaged in cyber security training without the pilot and 26 to 33 candidates would not be employed in cyber security. **The bases for both surveys are low, therefore, these figures are indicative.**

[55] *THIS IS BASED ON INFORMATION FROM 4 PROJECTS, THE REMAINING 3 DID NOT RECORD CANDIDATES' ETHNIC BACKGROUND*


CSIIF has successfully enabled 7 providers to develop, scale up or refocus their cyber security retraining projects.
To date 478 people have taken part in the pilot and 44 people have been placed into employment (16.8% of those who have complete their training).
This results in an estimated achieved net benefit which exceeds the total costs of the project

5. CONCLUSIONS AND RECOMMENDATIONS

5.1 Overview

This section sets out the conclusions and recommendations of this evaluation.

5.2 Conclusions

This evaluation set out to answer the research questions in Table 5.1.

Table 5.1: Research questions

Research questions	Conclusions
Is CSIIF an effective[56] form of government intervention that succeeds in its aim of stimulating the market to build an immediate route into the cyber security talent pipeline?	CSIIF has successfully enabled 7 providers to develop, scale up or refocus their cyber security retraining projects. To date 478 people have taken part in the pilot and 44 people have been placed into employment (16.8% of those who have completed their training). This results in an estimated achieved net benefit which exceeds the total costs of the project.[57]
Are the sponsored projects an effective method (for the candidate, the employer and the market) of retraining and upskilling candidates in the immediate term for an entry-level cyber security role?	Evidence from consultations with CSIIF providers and sector representatives and the results of the beneficiary survey indicates that the sponsored projects are an effective method[58] of retraining and upskilling candidates across a range of technical skills.

[56] *In this context, 'effective' is considered as the benefits of the Fund outweighing its costs.*
[57] *Assuming 70% of the candidates placed into employment were not employed prior to taking part in CSIIF and all remain in paid employment within the cyber security sector for at least 1 year.*
[58] *for the candidate, the employer and the market.*

5.3 Recommendations

Based on the findings of this evaluation it is recommended that *DCMS continues the Cyber Security Immediate Impact Fund until the identified market failures are addressed*. This evaluation also proposes the following recommendations to improve the impact of CSIIF in the future.

1. *Future initiatives should consider supporting the continued professional development of entry-level cyber professionals, as well as providing training for new entrants, to keep their skills relevant to the needs of the sector.*

2. *DCMS should advertise future funding opportunities further in advance and with a wider group of providers to encourage more diverse proposals. This would also give providers more time to engage employers and referral agencies in the development of their proposals, resulting in them setting more informed and realistic targets and timeframes.*

3. *Financial reporting requirements for projects and verification of spend by DCMS should include match funded expenditure. DCMS should also ask projects to submit a declaration of match funding at least once a year.*

4. *DCMS should establish a clear definition of the type of employment it intends candidates to be engaged in within 6 months of completing their project.*

5. *Providers indicate that the lead in time required for some projects was longer than expected. This should be factored into future funds to help set more realistic timeframes and targets.*

6. *The full benefits of this pilot will take longer to materialise than was originally expected. DCMS should continue its support of these projects to make sure that the momentum built up by its initial investment is not lost in the medium term whilst projects are securing their sustainability in the long term. This support could take the form of bridge funding, where appropriate, but also employer education. One of the main challenges' projects have faced is educating employers about how to support diversity and inclusion. This is an area where DCMS is well placed to intervene by recognising those who are doing it well and sharing examples of good practice and lessons learned from CSIIF on how to support the recruitment and retention of target groups.*

7. *DCMS, the NCSC and CSIIF providers could do more to reinforce the idea that the people participating in these projects are leading the direction of travel for cyber security.*

8. *DCMS should work with projects to gain participant consent to take part in longitudinal research into beneficiary outcomes (over the next 3 to 5 years) so that the full benefits of the pilot can be measured. If this is done by creating some form of CSIIF alumni group, it could also support the achievement of Recommendation 7.*

APPENDIX A: CSIIF PROJECTS

APPENDIX A: CSIIF PROJECTS

6.1 Introduction

The CSIIF pilot funded 7 projects. Each is described in turn below based on information collected from the CSIIF grant agreements.

6.2 CompTIA: Cyber Ready

6.2.1 Overview

CompTIA's Cyber Ready initiative aims to provide a new route for employers to get access to nascent cyber security talent from a diverse spectrum.

Cyber Ready has been developed to provide a replicable and scalable model for taking individuals with some IT Experience and adding additional training and certification over a 6 month period so that employers would recognise graduates of the project as being competent to perform in entry-level cyber security roles, such as a Cyber Security Analyst.

6.2.2 Target outcomes

- increased diversity in the workforce
- new route to market for existing IT professionals excluded by personnel circumstance
- improved perception of career opportunities
- greater supply of talent to close cyber skills gap
- improving UK plc's standing in global cyber capability
- encouraging diverse candidates to undertake this project

6.2.3 Agreed delivery milestones/ objectives

- engage with a minimum of 50 employers
- recruit 30 individuals. 30% of the candidates to be women (17% currently within the industry) - July 2018
- graduate rate of more than 80% - January 2019
- place all graduates into cyber security jobs
- charge organisations a set fee per candidate to secure the services on a Cyber Ready graduate - March 2019

6.2.4 Expected beneficiaries

The project will encourage and identify candidates that are from diverse backgrounds including BAME, women and neuro-diverse candidates.

Cyber Ready will be predominantly delivered online to allow a more flexible approach to learning. This will help individuals who have other commitments to participate. This would include:

- returnees to the workforce who have some prior IT experience (e.g. mothers, fathers, carers etc.)
- people working in a different sector but maybe IT hobbyists
- individuals working in first line IT roles and looking to develop
- recent graduates
- former IT Apprentices who are looking to gain new skills
- ex-service personnel

6.3 Immersive Labs: Neurodiversity Digital Cyber Academy

6.3.1 Overview

The Immersive Labs' Neurodiversity Digital Cyber Academy (DCA) initiative aims to upskill 1,000 people with neurodiverse conditions and encourage those who have developed cyber skills to apply for jobs, without unconscious bias, increasing diversity in the industry.

6.3.2 Target outcomes

1,000 people with neurodiverse conditions who have chosen to find out more about cyber security and a high volume of people with a broad range of cyber security skills and who are ready for entry-level roles in cyber security. This will all be evidenced through the Neurodiversity DCA. Candidate progress through DCA will be tracked, which includes the labs they have completed and the numbers who have applied for and been successful in securing a placement or role through the Academy.

6.3.3 Agreed delivery milestones/ objectives

- identify partners who will distribute access codes to neurodiverse individuals. The partners will evolve as the project continues - June 2018
- use the underlying Digital Cyber Academy technology for students and create the Neurodiversity DCA including website and content - June 2018
- add new platform technology that allows code-based access for individuals - June 2018
- source adverts from employers who are willing to sponsor it and employ neurodiverse candidates - June 2018
- create press/ marketing content and promote the new Academy - June 2018
- manage the Neurodiversity DCA and user experience - December 2018
- analyse the success of the pilot and share success stories - January 2019

6.3.4 Expected beneficiaries

- anyone in England with a recognised neurodiverse condition that is connected with a charity, academic institution or social enterprise and who is interested in developing cyber security skills
- employers who can recruit a diverse talent into the enterprise without unconscious bias
- UK economy through having a greater number of individuals in employment where a critical shortage exists

6.4 National Autistic Society (NAS): NAS Enterprise Cyber Security Programme

6.4.1 Overview

The NAS Enterprise Cyber Security Programme aims to demonstrate how the representation of neurodiverse candidates (both male and female) in the cyber security industry can be improved, addressing the underrepresentation of these 2 groups in the profession. It will (a) prepare young people for apprenticeships and (b) work with employers to make them more accessible to autistic candidates.

6.4.2 Target outcomes

- candidates in the programme will be prepared and supported to enter paid employment in the cyber security industry
- improved understanding in the sector of the talents these candidates bring, and the support/ adjustments needed to enable more diverse recruitment
- establishment of sustainable NAS cyber security programme delivering a pipeline of students who are apprenticeship-ready

6.4.3 Agreed delivery milestones/ objectives

- 12 young autistic people (25% female) entered into the programme - June 2018
- 12 employers offering apprenticeships and completing autism training - October 2018
- at 12 months, 50% of candidates will have secured apprenticeship positions - May 2019
- evaluation summary report detailing candidate outcomes and development plan (covering sustainability and potential for scale-up) – disseminated through networks and presented at conferences - May 2019

6.4.4 Expected beneficiaries

Primary beneficiaries will be:

- 12 young people on the autistic spectrum (male and female, aged 16-24) from Greater London and Essex
- 12 cyber security firms with improved capacity to benefit from the skills of a more neurodiverse workforce

Secondary beneficiaries will be:

- autistic people outside the programme benefiting from improved opportunities through potential scale-up of the programme and learnings for the sector
- the cyber security sector benefiting from improved understanding and awareness about autism.

6.5 PGI: Cyber Academy

6.5.1 Overview

PGI's Cyber Academy initiative aims to quickly create cohorts ready for employment as cyber security professionals who are then trained - funded by the employers - in the skills needed to perform cyber roles.

6.5.2 Target outcomes

- a female cohort employed and accepted into careers as cyber professionals - March 2019
- research on the gender specific barriers that prevent women from retraining/ upskilling into a career in cyber security from a non-cyber background

6.5.3 Agreed delivery milestones/ objectives

- creation of stakeholder network of organisations who can identify candidates - June 2018
- employers forums to build further buy-in to the project methodology - July 2018
- marketing, PR and recruitment process - September 2018
- employment and training programme - January 2019
- research report on the process - April 2019

6.5.4 Expected beneficiaries

- women candidates that are successfully trained and employed in cyber security roles
- organisations employing women candidates to increase diversity of their workforce

6.6 The Integrate Agency Community Interest Company (CIC): Cyber Safe Lambeth

6.6.1 Overview

The Integrate Agency CIC Cyber Safe Lambeth aims to create a thriving community of cyber security expertise in Lambeth.

6.6.2 Target outcomes

- 48 local single mothers, that the Integrate Agency CIC will source in Brixton, will attend a Certified Information Systems Security Professional cyber security training. Each course will feature a small group of 12 and there will be 4 of these 4 day courses

- all project attendees will be part of an Integrate-led network of alumni through a Facebook or LinkedIn page and the community will be encouraged to speak at local forums and events to promote the project and be role models to inspire others to cyber security careers
- Integrate will also develop a cyber security consultancy model based on the Digital Mums model and maintain the community they create through which to sustain the project.

6.6.3 Agreed delivery milestones/ objectives

- 16 March 2018
  - informed application was successful
  - leverage partners and network to begin engagement with project cohort in Brixton
  - training materials procured
  - room bookings formally agreed
- 30 April 2018
  - launch event at Lambeth Town Hall with first cohort of #CyberSafeLambeth
  - first training programme begins (30 April to 3 May)
- 7 May 2018
  - second training programme begins (7 May to 10 May)
- 14 May 2018
  - third training programme begins (14 May to 17 May)
- 21 May 2018
  - fourth training programme begins (21 May to 24 May)
- 4 June 2018
  - enterprise programme launched (4 June to 5 June)
    July
  - Hire A Volunteer launched providing practical, hands on opportunities to provide cyber security consultancy.
- September 2018
  - #CyberSafeLambeth start-ups and consultancies launched with events at Lambeth Town Hall and Battersea Power Station Village Hall
- October 2018
  - launch of Cybersecurity Digital Mums

6.6.4 Expected beneficiaries

- 10 exceptional attendees from the 48 will be selected for a cyber security enterprise programme, held over 2 days at Lambeth Town Hall
- each will receive a Battersea Power Station Foundation grant to seed-fund their cyber security business or professional development. The boot camp will work towards business plan development for start-up and/ or self-employment and support those seeking cyber security employment to plan their career paths. This group will be supported in executing their business and career plans by Integrate and introduced to local businesses by Lambeth Council, Battersea Power Station and the Young Lambeth Cooperative network.

6.7 UK Cyber Security Forum CIC: Community Security Operations Centre (SOC)

6.7.1 Overview

The UK Cyber Security Forum CIC's Community SOC initiative aims to place neurodiverse individuals in cyber security jobs and ensure they remain in these jobs, increase number of employers considering neurodiverse individuals for job roles and prevent neurodiverse candidates from committing online crimes.

6.7.2 Target outcomes

- neurodiverse individuals given relevant training and experience in cyber security skills. This would mean a new pool of individuals to fill the cyber security skills shortage
- neurodiverse individuals helped to develop a set of coping strategies to understand a workplace environment. The SOC will maintain mentorship with them for at least 3 months after they start working for a company. This will ensure that neurodiverse individuals will stay in the job
- education of local employers about neurodiversity. Includes inviting the local employers to workshops and arranging trips to commercial companies. This means that employers can utilise an additional pool of people to help solve cyber security skills gaps and their company becomes more innovative due to more diversity
- train individuals at risk of committing crime and referred to the SOC by the police. Give these individuals workplace skills and understanding to prepare them for commercial jobs. This would have an outcome of less computer crime

6.7.3 Agreed delivery milestones/ objectives

- confirm the first cohort of neurodiverse individuals - 9 April 2018
- buy the computers required to start the training sessions - 16 April 2018
- start the training and mentoring sessions 2 days per week - 23 April 2018
- people from at least 10 different companies visit the training and mentoring sessions - 30 June 2018
- arrange for the cohort to visit at least one commercial company - 30 June 2018
- the Community SOC will start a paid service offering - 31 August 2018
- five neurodiverse individuals will be ready to start apprenticeships - 30 September 2018
- two neurodiverse individuals will start an apprenticeship, employed by a commercial company - 30 September 2018
- delivery of a report which documents the progress against the aims of the project and any learning points - 30 September 2018

6.7.4 Expected beneficiaries

- individuals who gain employment and the employers who need these skills
- neurodiverse individuals have more employment opportunities and the employers who have a more diverse workplace

6.8 Youth Fed: Cyber Threat Hub Academy, Salford

6.8.1 Overview

The Youth Fed Cyber Threat Hub Academy aims to provide operational work experience in cyber security for those showing aptitude and interest in the profession whilst supporting national threat analysis activity. Specifically, the initiative aims to:

- build a pipeline of cyber security talent to enter the profession within 6 months of placement
- provide candidates with a defined career path
- provide local solutions to the cyber security skills deficit across the North West of England
- provide a replicable and sustainable solution for the UK where there is a professional support network in place

6.8.2 Target outcomes

- 150 beneficiaries pass through a newly created SOC training academy - May 2019
- 100% of candidates have opportunity to receive at least 30 hours of SOC work experience
- 80% of candidates equipped and more confident to obtain employment in the cyber industry as a result of the project
- 80% of candidates into cyber security education, apprenticeships or employment within 6 months of SOC experience.

6.8.3 Agreed delivery milestones/ objectives

- create a SOC training academy in Salford - May 2018
- instigate a 'satellite cyber threat hunting lunchtime club' at the Together Trust, Inscape House School for neurodiverse students to feed into Salford SOC - June 2018
- provide 150 individuals with 30 hours of professional cyber work experience each between June 2018 and June 2019
- provide opportunity for 6 weeks of pre 'Cyber First' holiday programmes for girls and young people showing 'latent talent' as identified by Youth Fed NW Cyber Programmes - June 2018
- contribute to threat intelligence on a national basis through other SOC Academies (1 based in Essex and a further 3 in the North West)

6.8.4 Expected beneficiaries

Primary beneficiaries:

- of the 150 beneficiaries that pass through the SOC and gain work experience, 80 will be female and/ or 50 will be neurodiverse
- 40 Inscape House neurodiverse students will engage in the project through the lunchtime 'cyber threat hunting clubs'

Secondary beneficiaries:

- additional beneficiaries: 30 Masters or PhD students from University of Manchester will support the SOC on a rota basis as part of their course requirements

APPENDIX B: PARTICIPANT SURVEY

APPENDIX B: PROFILE OF SURVEY RESPONDENTS

7.1 Overview

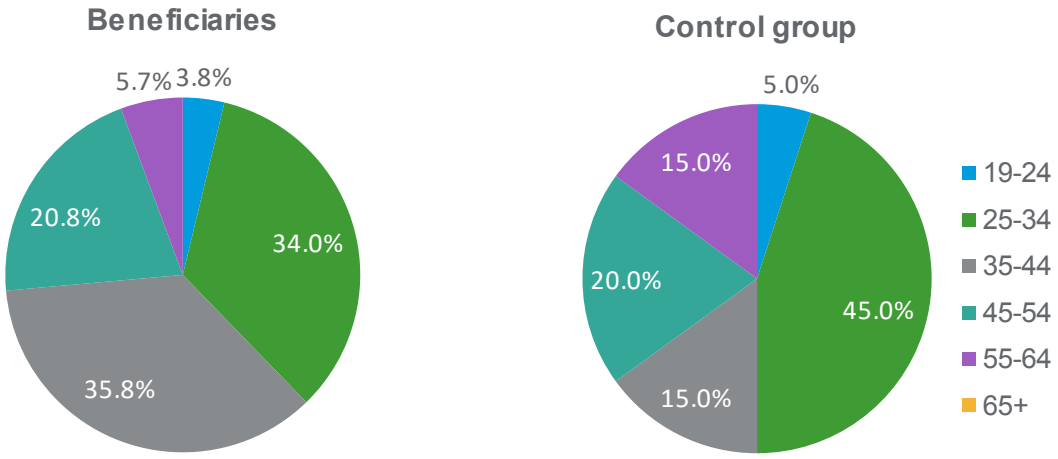
Two online surveys were developed to gather the views of people who applied to a CSIIF funded initiative. Due to data protection and GDPR regulations links to both surveys were distributed via CSIIF providers to:

- beneficiaries – *people who participated in a CSIIF project (achieving 54 responses or 18.9% response rate)*[59]
- a control group – *people who applied for a CSIIF project but who's application was declined (achieving 20 responses or 58.8% response rate)*[60]

This approach has skewed the profile of respondents resulting in 74.1% respondents to the beneficiary survey still participating in their CSIIF training.

7.2 Demographic Profile

Figure 7.1: Age of respondents



BASE: 53

BASE: 20

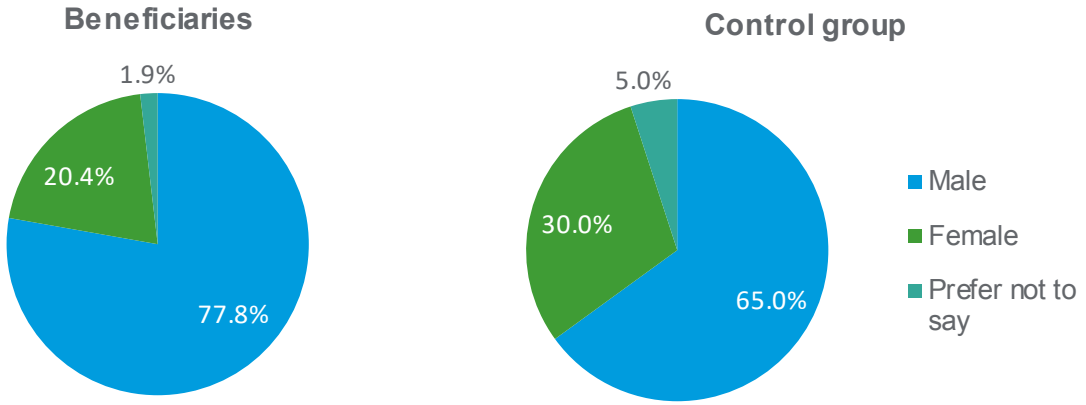
[59] *TOTAL POPULATION OF 285 (478 CANDIDATES LESS CANDIDATES FROM YOUTH FED (187), PGI (0) AND NAS (6)). YOUTH FED, WAS UNABLE TO DISTRIBUTE THE SURVEY LINK AS IT DOES NOT HOLD CONTACT DETAILS FOR ITS CANDIDATES. IT WAS ABLE, HOWEVER, TO SHARE FEEDBACK IT HAD COLLECTED FROM 60 CANDIDATES. DUE TO THE TIMING OF THE SURVEYS IT WAS AGREED WITH DCMS THAT ANY CANDIDATES FROM PGI AND NAS WOULD NOT BE SURVEYED. 54 RESPONSES GIVES A RESPONSE RATE OF 18.9%, WHICH IS REASONABLE FOR AN EXTERNAL ONLINE SURVEY ADMINISTERED VIA A THIRD PARTY. HOWEVER, DUE TO THE RELATIVELY LOW POPULATION, THE MARGIN OF ERROR FOR THIS SURVEY IS RELATIVELY HIGH (± 12% AT THE 95% CONFIDENCE LEVEL). THIS MEANS THAT THE SURVEY FINDINGS ARE INDICATIVE AND SHOULD NOT BE GENERALISED TO REPRESENT THE WHOLE POPULATION.*

[60] *TOTAL POPULATION OF 34 (878 APPLICANTS TO DATE MINUS 285 CANDIDATES AND APPLICANTS FROM YOUTH FED (187), PGI (360) AND NAS (12)). 20 RESPONSES GIVES A RESPONSE RATE OF 58.8%, WHICH IS GOOD FOR AN EXTERNAL ONLINE SURVEY ADMINISTERED VIA A THIRD PARTY TO UNSUCCESSFUL APPLICANTS. HOWEVER, DUE TO THE RELATIVELY LOW POPULATION, THE MARGIN OF ERROR IS RELATIVELY HIGH (± 14% AT THE 95% CONFIDENCE LEVEL). THIS MEANS THAT OUR SURVEY FINDINGS ARE INDICATIVE AND SHOULD NOT BE GENERALISED TO REPRESENT THE WHOLE POPULATION.*

As shown in Figure 7.1, over two thirds (69.8%) of respondents from the beneficiary survey were aged 25 to 44. A further 20.8% were aged 45 to 54 while only 5.7% were aged 55 to 64 and 3.8% aged 19 to 24. The age breakdown of the beneficiary group was similar to the control group, where 60% of respondents were aged 25 to 44, 20% were aged 45 to 54, 15% were aged 55 to 64 and only 5% were aged 19 to 24.

As shown in Figure 7.2, the majority of respondents (77.8%) from the beneficiary survey were male while only 20.4% were female and 1.9% preferred not to state their gender. This is in line with the gender breakdown of the control group, where 65.0% were male, 30.0% female and 5.0% preferred not to say.

Figure 7.2: Gender of respondents

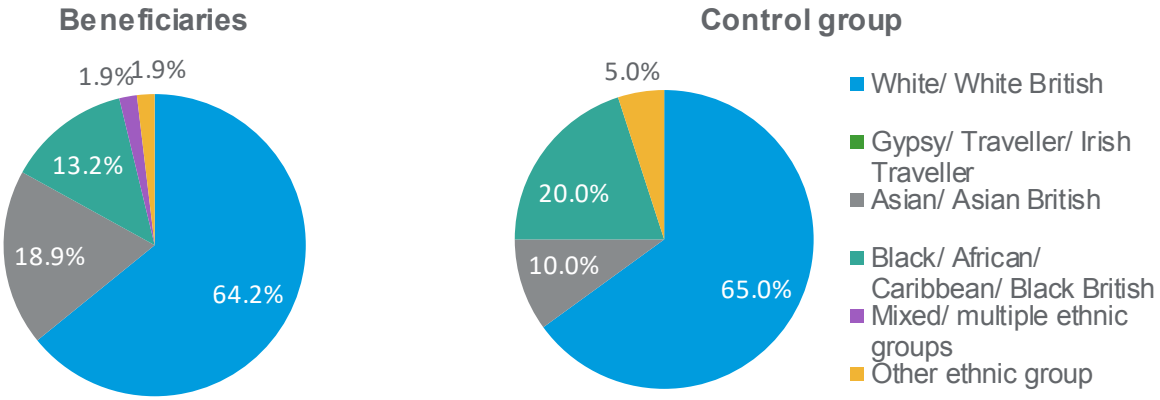


BASE: 54

BASE: 20

As shown in Figure 7.3, almost two thirds (64.2%) of respondents from the beneficiary survey were White/ White British. This ethnicity composition is similar to the control group, where 65.0% of control survey respondents were White/ White British. 18.9% of the beneficiary respondents were Asian/ Asian British compared to 10.0% within the control group.

Figure 7.3: Ethnicity of Respondents



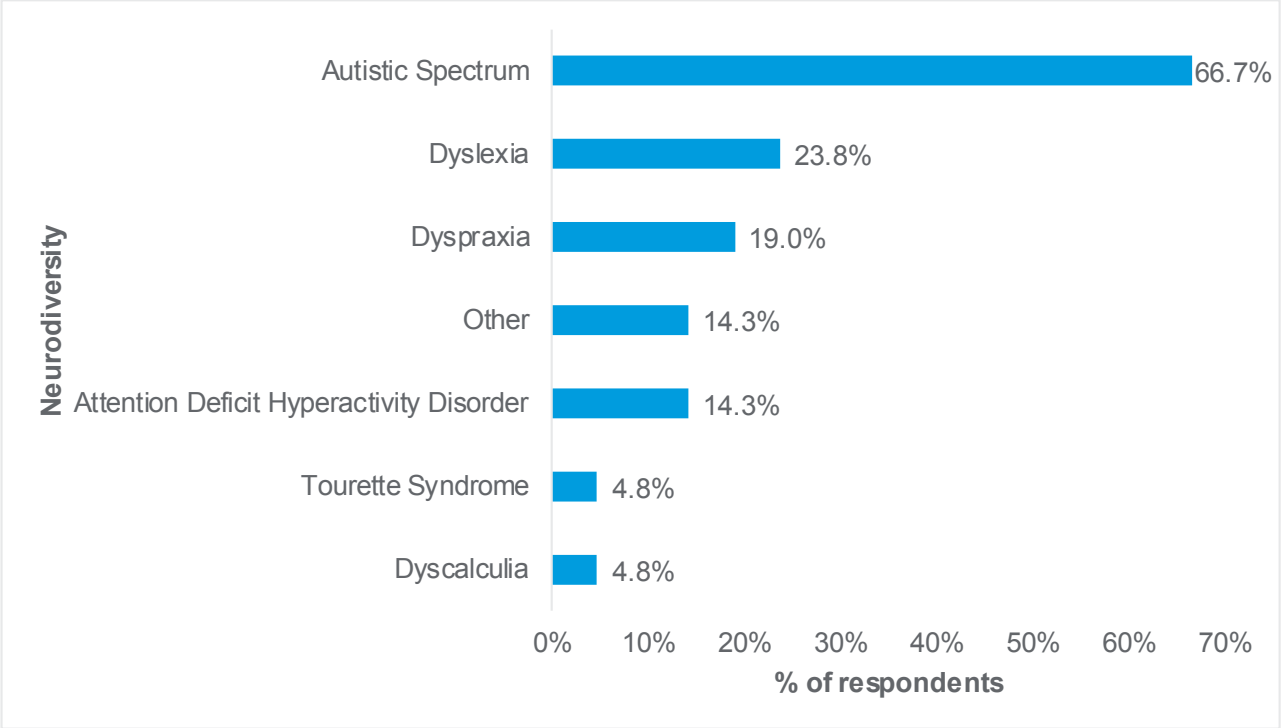
BASE: 53

BASE: 20

Neurodiversity is the variation and differences in neurological structure and function that exist among human beings. 38.9% of respondents to the beneficiary survey had at least one neurodiverse condition. As shown in Figure 7.4, when asked about their neurodiversity, 66.7% of those who were neurodiverse stated that they were on the autistic spectrum while 23.8% stated that they had dyslexia and a further 19.0% had dyspraxia. The 'other' option included one respondent who said they had borderline dyslexia, another that suffered from social anxiety and a third who declined to state their condition.

Six respondents (11.8% of those who answered this question and 28.6% of those with neurodiverse conditions) stated that they had 2 or more of the conditions outlined in Figure 7.4.

Figure 7.4: Beneficiaries with Neurodiverse conditions



BASE: 21

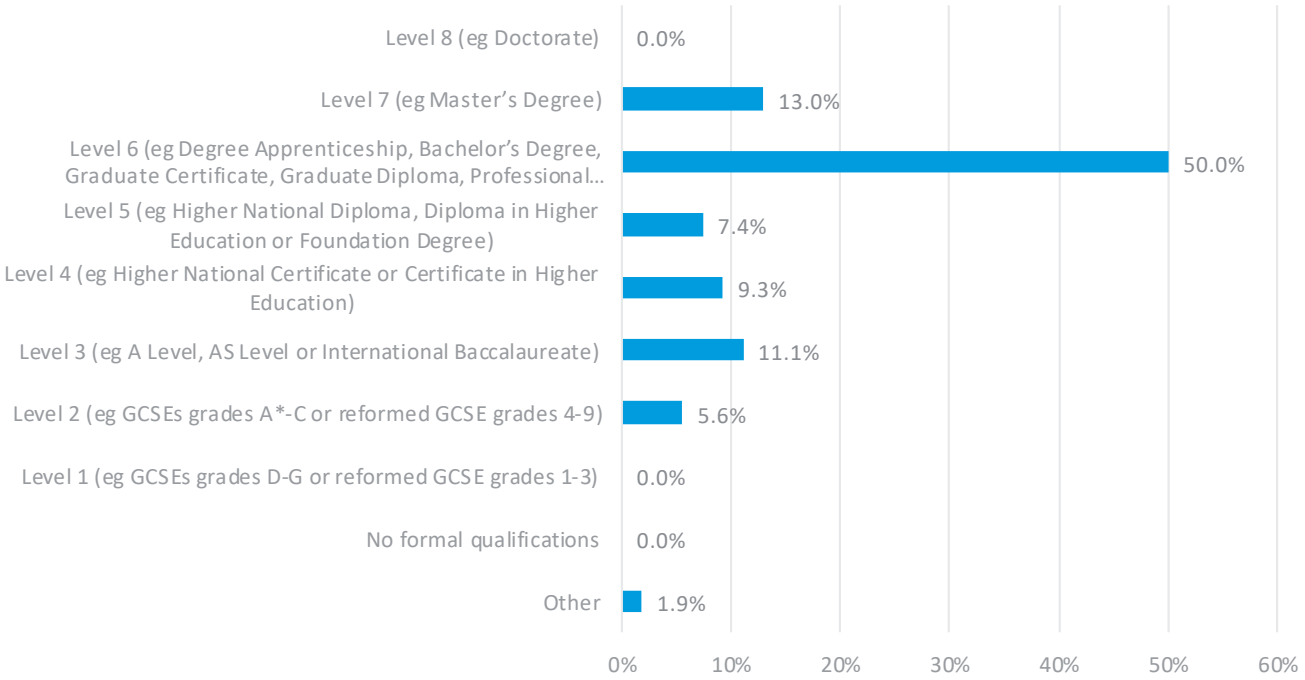
NOTE: THIS QUESTION ALLOWED FOR MULTIPLE RESPONSES. 21 RESPONDENTS INDICATED A TOTAL OF 31 CONDITIONS

The majority of respondents within the control group (84.2%) stated that the question was not applicable to them. Two respondents (10.5%) stated that they had dyslexia (one of which also had dyscalculia), one respondent (5.3%) stated that they had dyspraxia and one (5.3%) stated that they were on the autistic spectrum.

7.3 Education

Figure 7.5 shows the highest level of qualification that the beneficiary respondents had gained prior to applying for the cyber security project.

Figure 7.5: Level of Qualification – Beneficiaries



BASE: 54

OTHER: PROFESSIONAL QUALIFICATIONS (I.E. LPIC-1, SECURITY+)

Figure 7.5 highlights that 7 respondents (13.0%) from the Beneficiary Survey had a Level 7 Qualification prior to applying for the cyber security initiative whilst a further 27 (50.0%) had a Level 6 Qualification. 15 respondents (27.8%) had Level 3-5 Qualifications.

Of the control group, 6 (30.0%) had a Level 6 Qualification whilst 9 respondents (45.0%) had a Level 7 Qualification. Four respondents (20.0%) had Level 3-5 whilst 1 (5.0%) had a Level 8 Qualification.

All of the respondents (beneficiary and control group) had achieved at least a Level 2 Qualification prior to applying to the project.

rsmuk.com