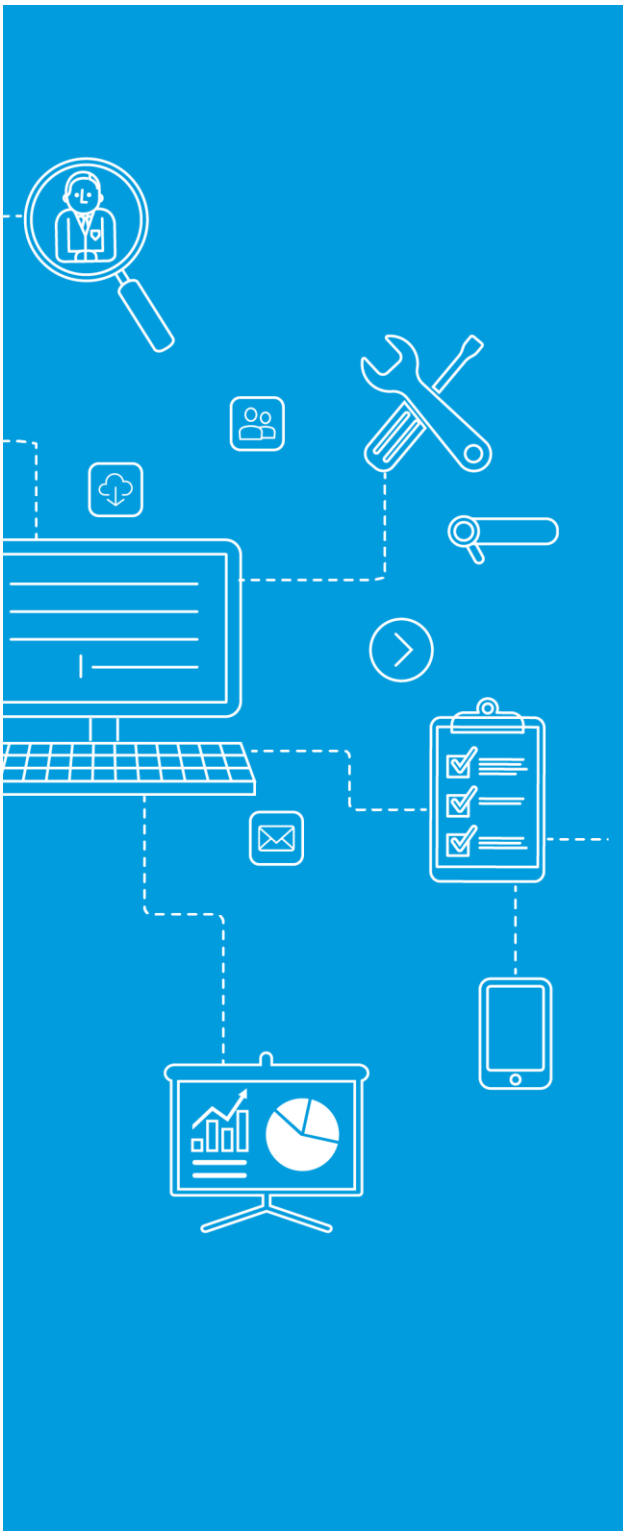


EVALUATION OF CYBER CRITICAL NATIONAL INFRASTRUCTURE APPRENTICESHIPS PROGRAMME AND OTHER INTERVENTIONS IN THIS SPACE - FINAL REPORT

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

September 2020

Fieldwork period – February / March 2019 and July - August 2019
Report completed – September / October 2019

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

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

CONTENTS

1. EXECUTIVE SUMMARY

1.1 Context / background to the programme

As part of the national cyber security strategy (NCSS) the Department for Digital, Culture, Media and Sport (DCMS) invested in piloting 2 cohorts of learners in the cyber critical national infrastructure (CNI) apprenticeships programme. This focused on the level 4 cyber security technologist standard over the period 2017 – 2019.

The cyber CNI apprenticeship programme was set up specifically to help encourage the uptake of apprenticeships in the wider economy and specifically in the CNI sectors. This corresponds with the DCMS objective to ensure there is a sustainable supply of home grown skilled cyber professionals to meet the growing demand of an increasing digital economy.

1.2 Research Objectives

In November 2018 DCMS appointed RSM UK Consulting LLP to evaluate the cyber CNI apprenticeship programme. This report summarises the key findings from both cohorts against the overall research objectives:

- understand how the CNI cyber apprenticeships scheme performed and was aligned to the original vision
- evaluate and understand the overall success of the scheme
- understand the barriers to employment in the CNI cyber industry specifically and in the wider economy
- understand where government policy may hinder apprenticeships in cyber space or where government could do more
- understand views from across the cyber industry on apprenticeships, training providers and looking at other successful apprenticeships initiatives
- propose other options for running a future cyber apprenticeship scheme (or alternative scheme in the Higher/Further education space) (including costings) that could be run by government, considerations for any policy implementations or scheme that could be run by the wider cyber industry

The aim of this evaluation is to inform government's future approach to addressing the need for an immediate path into the cyber security profession. **Note:** 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.

1.3 Limitations to our research

There were several limitations for our research, namely:

- **lack of robust data on the cyber security skills gap in the CNI sector** – there is limited data on the number of vacant cyber security roles and the type of cyber security resources companies in the CNI sector require or at what level. Research available on the skills gap refers to basic and high-level skills however it does not map to the apprenticeship standards

- **lack of evidence on the uptake and benefits of the cyber security standards** – the level 4 cyber security apprenticeship standard was only approved for delivery in 2017 and the level 6 and level 7 standards in 2018, therefore it may take time to stimulate interest. Promotion of the benefits when more evidence is available is one way to achieve this
- **timing of the evaluation** – apprentices are still completing the programme and therefore confirmed outputs (e.g. those that pass the end point assessment) as well as outcomes for the learner or company once the apprenticeship is complete are not yet known for some
- **apprenticeship levy** – the levy was introduced in April 2017 and a recent House of Commons briefing paper on apprenticeships and skills policy in England[1] notes that some employers have found it difficult or too complex to implement.[2] The levy was not in place at the start of cohort 1 however employers were aware that it was planned. It impacted on cohort 2 employers however this research does not explore the extent to which they would have used the levy funding anyway, or incurred the same training cost in the absence of the programme
- **insufficient number of apprentices / employers on the programme, leading to low survey and interview responses** – there were a small number of companies involved and only a subset of these choose to participate in the evaluation. Therefore, the findings are only indicative and should be treated with caution
- **lack of international data** – key developments in addressing the cyber security skills gaps in other countries (United States (US), Israel, Australia, Singapore) as well as other devolved nations within the UK were examined, however none of the other countries reviewed had progressed significantly more than the UK in relation to addressing the cyber security skills gap or in implementing cyber security apprenticeships

1.4 Conclusions and Recommendations

This section outlines conclusions based on the evidence collected and recommendations to inform other programmes in this area.

Note - caution should applied to all survey findings due to the small number of responses. The findings in this section are based on feedback from:

- survey of apprentices (n=19)
- interviews with CNI employers who participated in the programme (n=9) and 2 who completed the CNI employer survey
- the non-participating employer survey (n=14) (companies who were contact by DCMS to participate in the programme however declined to do so at that stage)
- strategic stakeholder interviews (n=34)

[1] Powell, Andrew (2019) Apprenticeships and skills policy in England

[2] EEF (2019) A Levy Price to Pay? The Apprenticeship Levy One Year On

1.4.1 State of the sector and market failures

a) Lack of company awareness of the cyber security skills needed

The cyber security skills requested by companies vary depending on awareness of cyber security risks; awareness of cyber security skills or roles; and willingness to invest in an appropriate resource or support for their need.

There is a lack of detailed evidence on what cyber security skills are needed by companies in the CNI sectors. The information that exists focuses on basic and high-level skills, however this is not directly linked to the apprenticeship standards. There is also evidence that some companies are not clear on how to assess their cyber security skill needs or how best to fill these.

b) Employment of cyber security apprentices

Recent research[3] notes the prevalence of cyber apprenticeships across the private, public and charitable sectors is relatively low. Interviews completed with employers, professional bodies and training providers as part of this research indicate that many companies are unclear of the benefits of apprenticeships in this specific area.

A recent report[4] by the Federation of Small Businesses (FSB) found that SMEs are critical to achieving the government's target of reaching 3 million new apprenticeships by 2020, however some smaller companies often lack the relevant cyber security skills and resources to recruit, train and supervise apprentices.[5] As a result they try to recruit staff with pre-existing technical skills.

Consultation feedback from one professional body and SME consultees (n=2) highlighted that SMEs may not be considering cyber security apprenticeships due to:

- resource / expertise needed - most do not have the support infrastructure they would need to put in place (the DCMS cyber CNI apprenticeship programme required each participating company to have a line manager and mentor for apprentices). In addition, SME consultees highlighted smaller companies may not be able to provide apprentices with sufficient breadth of experience to support the completion of their portfolio or the management time required to help them develop skills for everyday work (for example, time keeping as well as report writing, problem solving and interpersonal skills)
- financial cost - SMEs do not have the funding they would need to invest (e.g. to cover the apprentice and line manager time). One SME consultee also highlighted that the apprentice training time required could have an impact on the wider team if there were only a small number of cyber security staff working on a project
- lack of information / knowledge - SMEs may not know the skills they need, or the interventions available to address these

Given the importance of the CNI sector to the rest of the economy and society it is important that SME employers are helped to overcome these barriers.

[3] Ipsos Mori (2018) Understanding the UK Cyber Security Skills Labour Market

[4] Fit for the Future (2019) Making the Apprenticeship System Work for Small Businesses

[5] The report notes this was a problem for cyber apprenticeships rather than for general IT apprenticeships, where existing staff were more likely to have relevant skills and knowledge to impart.

Recommendation 1: There remains a need for government intervention to overcome the market failures and ensure cyber security skill objectives are met. The specific market failures are:

Information failure: many employers are not clear on what their cyber security skill needs are and / or how the level 4 apprenticeship fits with these.

Resource / expertise failure: SMEs often do not have the resource or systems in place to support apprenticeships.

Recommendation 2: We recommend that companies within the CNI sector are provided with information on the cyber security risks, the costs of not being ready to mitigate these and how having the right skills and capacity is essential to improve cyber resilience. Ideally case studies could be used to promote how cyber security skills and expertise benefit companies in the CNI sector.

Recommendation 3: We recommend that greater clarity is needed on the jobs and the skills needed by CNI companies and how they map to apprenticeship levels 3 to 7 (and beyond).

Recommendation 4: We recommend that specific supports are put in place to help SMEs access and support apprentices. Examples of good practice include the construction sector where almost three quarters of construction sector SMEs (73%) currently employ apprentices, which is higher than the proportion of SMEs employing apprentices across all sectors (65%).[6] Current initiatives include the CITB Shared Apprenticeship Scheme[7] which allows companies to take on an apprentice, for as short a duration as three months, with no commitment to the apprentice at the end. It allows employers to support and benefit from apprentices, even if they are unable to offer them a long-term placement.

Recommendation 5: We recommend that DCMS work with the Institute of Apprenticeships to ensure that SMEs, in the CNI sector particularly, are made aware of any new developments to support them engage with cyber security apprenticeships.

1.4.2 Success of the programme

Success of the programme is based on reviewing uptake levels, quality of delivery, project management and the outcomes achieved.

Uptake

Companies - the marketing of the programme to employers was limited to a ministerial letter[8] to companies in the CNI sectors alongside DCMS using their existing contacts with CNI employers and via working groups. This was initially focused on energy, transport and defence organisations and was expanded to include more sectors[9] for cohort 2. Feedback from participating companies suggests direct engagement was helpful in getting them involved, however this element of the

[6] https://www.showhouse.co.uk/news/nearly-three-quarters-of-construction-smes-employ-apprentices/ (accessed September 2019)

[7] https://www.citb.co.uk/courses-and-qualifications/citb-apprenticeships/take-on-an-apprentice/types-of-apprenticeships/shared-apprenticeship-scheme/ (accessed September 2019)

[8] 40 companies were initially contacted in autumn 2016 and an additional 100 were written to via a ministerial letter in 2017

[9] Expanded to include water, telecoms, cyber and media

programme was significantly under-resourced. The marketing of the programme needs to be more extensive, ensuring that more companies are informed of the programme, while also being given information on cyber security risks and the ways in which cyber security apprentices can address these. The introduction of levy funding in April 2017 also impacted on company involvement as DCMS stakeholder feedback noted companies often did not understand how it would work. As a result, companies were less keen to take on and invest in an apprentice at this stage in the levy implementation.

The timing of apprentice recruitment had a detrimental impact on both company and apprentice involvement. In cohort 1 the timing of the National Cyber Security Programme (NCSP) business case cycle meant a confirmed offer of support could not be given to employers before April 2017. Ideally offers would have gone out in early autumn 2016, when firms were completing their financial planning for the year ahead. In addition, it often takes time to equip companies with the knowledge to make decisions on new apprentices and they require a longer lead in time from initial contact by DCMS. For apprentices in cohort 1, feedback from the training organisation (QA) indicates the timing of the application process was also a key issue as the requirement for cohort 1 learners to be signed up by 24 April 2017 created a 'rushed process'.

Apprentices - there were a significant number of eligible apprentice applicants for both cohorts (1,024 in cohort 1 and 1,164 in cohort 2), resulting in 51 apprenticeships in total. Therefore, the current promotional activities for apprentices appear effective. However, the application process involved six stages[10] which may be disproportionate for the level of apprenticeship involved and may not work for both larger and smaller organisations as their recruitment processes will differ. The overall conversion rate (i.e. from completing the application form to offers being made) was 3% as due to the lower than anticipated number of employers, there were a limited number of apprenticeship places available. As a result, the original target of 150 new apprentice starts was not met. Data on the total number of candidates meeting the requirements to reach the final stage of the process was not available from the recruitment organisation within the timeframes of this project. Of the 51 apprentices who joined the programme 7 dropped out, resulting in an expected completion rate of 86%[11]. As apprentices are still completing their end point assessments, it is not yet possible to report a final pass rate for the programme.

Recommendation 6: We recommend that marketing materials setting out the benefits to employers of using cyber security level 4 apprentices are developed and made available to employers across the CNI sector.

Recommendation 7: We recommend DCMS consider involving the Digital Skills Partnerships in marketing programmes to local employers in their areas.

Delivery of training and support

Most participating employers that provided feedback felt that the training provided by QA[12] met the objectives of the learning and was of good quality, with one employer noting "apprentices felt they

[10] The selection process for the programme included: eligibility questions; application form; Capp's online assessment suite telephone interview; video interview; final assessment stage or assessment centre

[11] Based on 7 apprentices dropping out, it is estimated that 44 will complete the programme (44 / 51 = 86%)

[12] There are also several other training providers delivering the level 4 cyber security technologist standard

were getting good quality tutors who were able to help them and convey the material at the right level".

Moreover, both companies and apprentices felt that allocating time to training and learning on a weekly basis was more beneficial than assigning training time in larger blocks as it allowed for the learning to be applied on a more continuous basis. Of the 19 apprentices that provided feedback 95% (n=18) were satisfied or very satisfied with the time they had for training.

However, companies and apprentices highlighted a need for greater clarity on how the course content maps to the level 4 apprenticeship standard assessed by the British Computer Society (BCS) end point assessment. In addition, both employers and apprentices highlighted there was insufficient communication on progress of the apprentices against programme requirements, and employers felt that the regular meetings with the Skills Coaches[13] lacked sufficient structure and did not add value.

Recommendation 8: We recommend any future intervention should consider the learnings from this programme, including:

- content alignment – there is a need for greater clarity on how the course content, the BCS end point assessment and the level 4 cyber security technologist standard fit together
- support provided by Skills Coaches – in any future intervention the Skills Coaches should:
  - provide timely guidance and feedback in response to work or queries submitted
  - have clear roles and responsibilities (ideally measurable), the details of which is shared with employers
  - have a standardised approach to ensure face to face meetings between Skills Coaches, employers and apprentices provide sufficient and ongoing feedback (from both the employer and the Skills Coach) on how the apprentices are progressing against the expected standards as well as any gaps or issues outstanding and how to address these
  - receive feedback from employers on performance against their roles, responsibilities and performance measures

Project management

While general updates on the programme and learner progress were provided by QA to DCMS there was no centralised governance or formal, documented reporting against the measures set for performance. Companies also highlighted they would have liked greater governance and monitoring of the programme by DCMS as the funding body to manage the performance of the training provider and ensure quality.

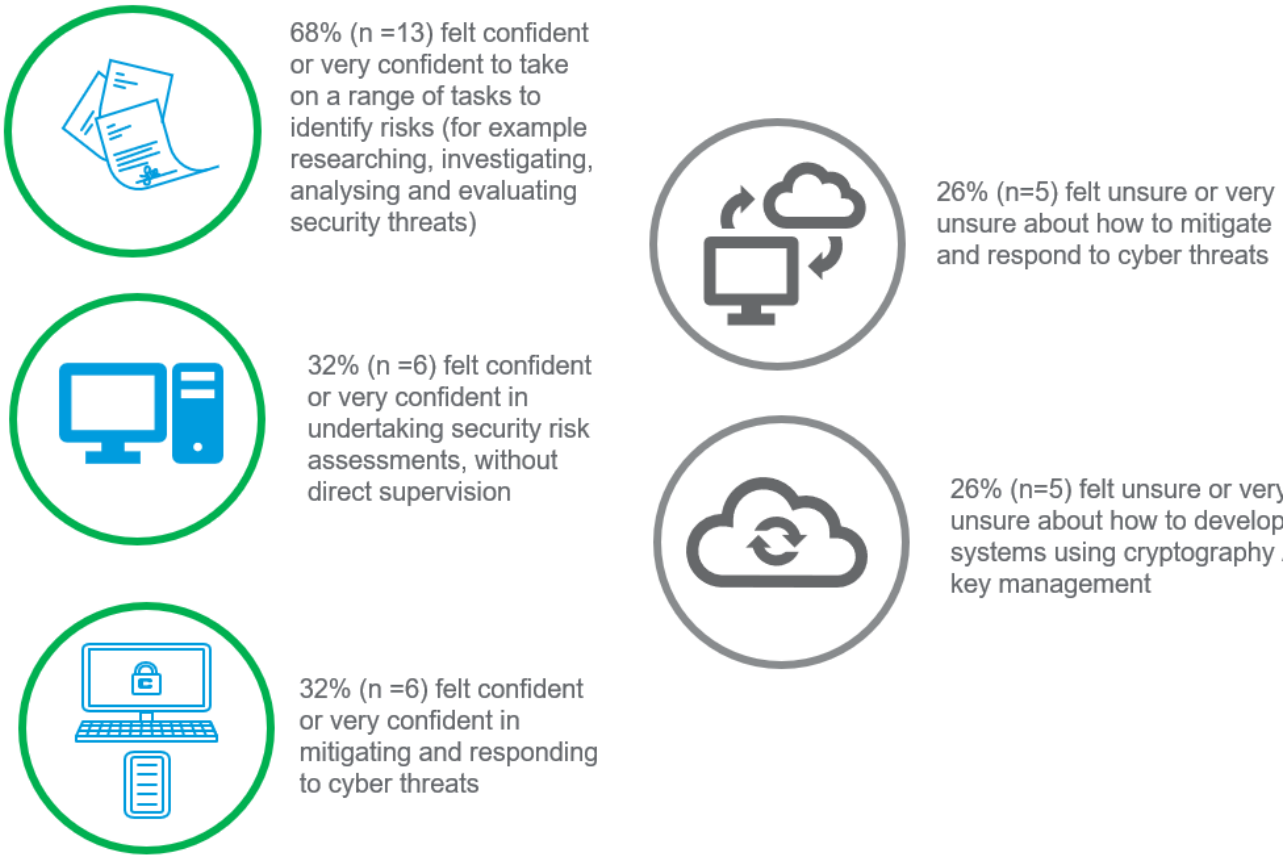
Recommendation 9: We recommend any future intervention should include the requirement for the training provider to submit regular progress reports to the funding organisation detailing performance against the agreed metrics as set out in the contract.

[13] QA Skills Coaches supported apprentices throughout the programme. They were responsible for: helping apprentices to build their portfolio as the programme progressed; meeting apprentices and their line managers regularly in the workplace to check their progress and provide support where needed; and providing pastoral care

Recommendation 10: We recommend any future intervention clarify the role and responsibilities of the sponsor, recruitment organisation and training provider to ensure those participating in the programme know what can be expected from each.

Outcomes achieved

Apprentices were asked to rate how confident they felt in several areas related to the role of a Cyber Security Technologist and respondents indicated that from a combination of course material and on the job training provided:



1.4.3 Other interventions and the way ahead

Four options were considered as potential interventions to provide a sustained supply of home-grown cyber security talent to help meet cyber security skills gaps in the UK and in particular the CNI sector:

- Option 1 (existing scheme - status quo) - involves a level 4 cyber apprenticeship programme for CNI sector companies
- Option 2 (level 6 cyber security technical professional or for the CNI sector) - this option was suggested by employers in the CNI sector and involves DCMS funding a level 6 cyber security technical professional degree apprenticeship
- Option 3 (level 4 cyber security apprenticeship for the non – CNI sector) - involves DCMS funding a level 4 cyber security apprenticeship for non - CNI sector companies to recruit new cyber security staff. The content would be the same as option 1 and is based on research that

shows high levels of basic technical skills gaps are more evident in the food or hospitality; construction; retail or wholesale; and professional scientific or technical firms[14]

- Option 4 (accredited tailored interventions to transition existing employees into new cyber security roles in the CNI sector) - this option was based on feedback from employers and involves DCMS providing funding for companies to retrain existing employees into new cyber security roles. The level of support required will depend on the skill gaps within individual companies / sectors

Preferred option

There are gaps in the information available and therefore insufficient data to make clear recommendations on which option would provide the best value for money.

Employer buy in is critical to delivering a cost-effective apprenticeship intervention in this space. However, as many companies are unclear as to their cyber security skill needs or how the apprenticeship levels fit with any needs they may have, employer demand is unclear. The piloting of different schemes and interventions allows companies the opportunity to trial new apprenticeship levels. Therefore, further evaluation work will be required to assess if they address the identified market failures in an effective way.

The UK cyber security market is embryonic and constantly changing. As a result, there is a need for apprenticeship supports to be piloted and tested, in order to build greater knowledge and evidence of employers' needs. This work is essential in order to build case studies on what works and use this to market apprenticeships with other employers to encourage uptake. Information on career pathways, jobs and how they link to apprenticeship standards and job / progression opportunities are all needed.

Delivery

The options outlined above could be delivered using an employer / industry led or a government led approach.

Government led approach – the cyber CNI apprenticeship programme used a 'government led' approach as DCMS were responsible for the management of the programme and provided a link between employers and the training provider. This approach also meant employers were 'recruited' onto the programme rather than companies seeking the type of apprentice that would meet their company's needs. While the government led approach was appropriate to try to stimulate the market to prioritise cyber apprenticeships, it meant less direct engagement between the employer and training provider than normally occurs in apprenticeship delivery and resulted in confusion on roles and responsibilities. Going forward, an alternative approach may be for government to focus on providing support to create a market demand for apprentices, rather than on the project delivery aspect or financial funding.

Employer led approach – an 'employer / industry' approach involves companies having responsibility for seeking the apprenticeships that fit with their company needs and directly contracting with the training provider.

[14] Ipsos Mori (2018) Understanding the UK Cyber Security Skills Labour Market

The advantages and disadvantages of each approach are set out below:

Approach	Advantages	Disadvantages
Government led approach	The approach used in the cyber CNI apprenticeship programme provided a pilot scheme where none previously existed, allowing companies to trial this when they may not otherwise have chosen the level 4 cyber security technologist standard.	Many employers (especially large employers) have apprenticeship systems / processes already in place and as a result prefer to liaise directly with training providers to ensure their needs can be met, rather than going through another organisation. The training provider is more easily able to focus on employer needs rather than metrics that often need to be included in a public sector contract to demonstrate accountability for public monies.
Employer led approach	Gives the employer greater responsibility and ownership of the training and the opportunity to develop relationships with the training providers. The importance of establishing a productive employer / trainer relationship is highlighted in recent research[15] on future skills challenges which noted that the linear model of 'education to employment to career' is no longer sufficient. Research[16] suggests that educators and employers need to collaborate more closely and develop new and innovative partnerships and flexible learning approaches, stating that "every effort must be made by government to adopt a whole-skills approach and to embed educator –employer partnerships across policy to support this".	It relies on employers being sufficiently motivated and knowledgeable on how the apprenticeship programme can help their business for them to consider this as an option.

Employers that participated in the cyber CNI apprenticeship programme and provided feedback suggested they were willing to try different approaches to recruiting cyber security staff (i.e. graduates, other apprenticeships or training internal employees). The options above demonstrate that an employer led approach to increasing cyber security skills / resources is likely to be most effective on a large scale, with the role of government as an enabler to support market demand. This could include stakeholder engagement and campaigns to raise awareness of the benefits of taking on and training an apprentice in cyber security.

Recommendation 13: We recommend the continuation of the test and learn approach being used by employers to cyber security apprenticeships in the CNI sector and the collation of evidence of what works and any learnings until the market develops.

Recommendation 14: We recommend that the UK should consider what current programmes (including the apprenticeship levy) could be promoted to employers or could be developed to transition existing employees into cyber security roles. In addition, as part of the cyber security skills strategy DCMS could consider detailing the steps employers can undertake to ensure effective workplace transitions.

[15] Universities UK (2018) Solving Future Skills Challenges

[16] Universities UK (2018) Solving Future Skills Challenges

2. RESEARCH OBJECTIVES AND METHODOLOGY

2.1 Research Objectives

In November 2018 DCMS appointed RSM UK Consulting LLP to evaluate the cyber CNI apprenticeship programme. This report summarises the key findings from both cohorts against the overall research objectives:

- understand how the CNI cyber apprenticeships scheme performed and was aligned to the original vision
- evaluate and understand the overall success of the scheme
- understand the barriers to employment in the CNI cyber industry specifically and in the wider economy
- understand where government policy may hinder apprenticeships in cyber space or where government could do more
- understand views from across the cyber industry on apprenticeships, training providers and looking at other successful apprenticeships initiatives
- propose other options for running a future cyber apprenticeship scheme (or alternative scheme in the Higher/Further education space) that could be run by government, considerations for any policy implementations or scheme that could be run by the wider cyber industry

The aim of this evaluation is to inform the government's future approach to addressing the need for an immediate path into the cyber security profession.

2.2 Methodology

The methodology used was agreed with the DCMS and the stages of work involved:

Project planning – development of an evaluation plan that incorporated a programme logic model, evaluation framework and methodology, outline of the consent process followed for apprentices and companies, governance arrangements and risk assessment.

Desk research and analysis – included a review of:

- relevant strategic and context documents (including the National Cyber Security Strategy 2016 to 2021, DCMS (2018), Initial National Cyber Security Skills Strategy, and Ipsos Mori (2018) Understanding the UK Cyber Security Skills Labour Market)
- performance information (including the number of applicants (apprentices and company), number of participants (apprentices and company), number of drop-outs, and number of completions)

Review of what is happening elsewhere (desk research and telephone interviews - overview of similar existing approaches to addressing the cyber security skills gap in other countries (United States (US), Israel, Australia, Singapore and the other devolved nations within the United Kingdom (UK)).

Consultations with strategic stakeholders – 33 interviews (face to face and telephone) were completed with:

- DCMS (Head of Cyber Security Skills Team)
- QA (Account Director and Skills Coaches (x2))
- Digital Skills Partnerships (x3: Head of the Digital Skills Partnership and Digital Skills Coordinators for Lancashire local Digital Skills Partnership and West Midlands Combined Authority)
- Institute for Apprenticeships
- Apprenticeship Standards Quality and Assessment, DfE
- three government representatives (two who were involved at the inception of the programme and one leading on another government level 4 apprenticeship scheme)
- industry bodies (Tech UK and Crest)
- professional bodies (IISP)
- Tech Partnership Degrees
- Qufaro
- IBM (chair of level 3 trailblazer group)
- National Cyber Security Centre (NCSC)
- National Apprenticeships Service
- company involved in developing the level 4 Cyber Security Cyber Security Technologist Standard*
- further and higher education institutions providing undergraduate and postgraduate cyber security courses (x10)
- second level education provider
- SMEs (n=1) / SME representative body (n=1)

* were consulted as part of the cohort 1 however their feedback was also relevant for, and has been used in, the development of this report.

Surveys and interviews with employers and apprentices – an online survey was distributed to all participating apprentices and companies as well as companies who were contacted by DCMS and decided not to take part in the programme. In addition, telephone interviews were completed with companies who provided consent to be contacted. In total the following was completed:

- survey of apprentices (n=19)
- interviews with CNI employers who participated in the programme (n=9) and 2 who completed the CNI employer survey

- the non-participating employer survey (n=14) (companies who were contact by DCMS to participate in the programme however declined to do so at that stage)

Reporting - the information gathered at each of the stages above were used to produce a draft and final report.

Note: 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.

2.3 Report Outline

The remainder of this report is set out as follows:

Section 3 – context

Section 4 – state of the sector

Section 5 – performance of cohorts 1 and 2

Section 6 – options and the way ahead

Section 7 – conclusions and recommendations

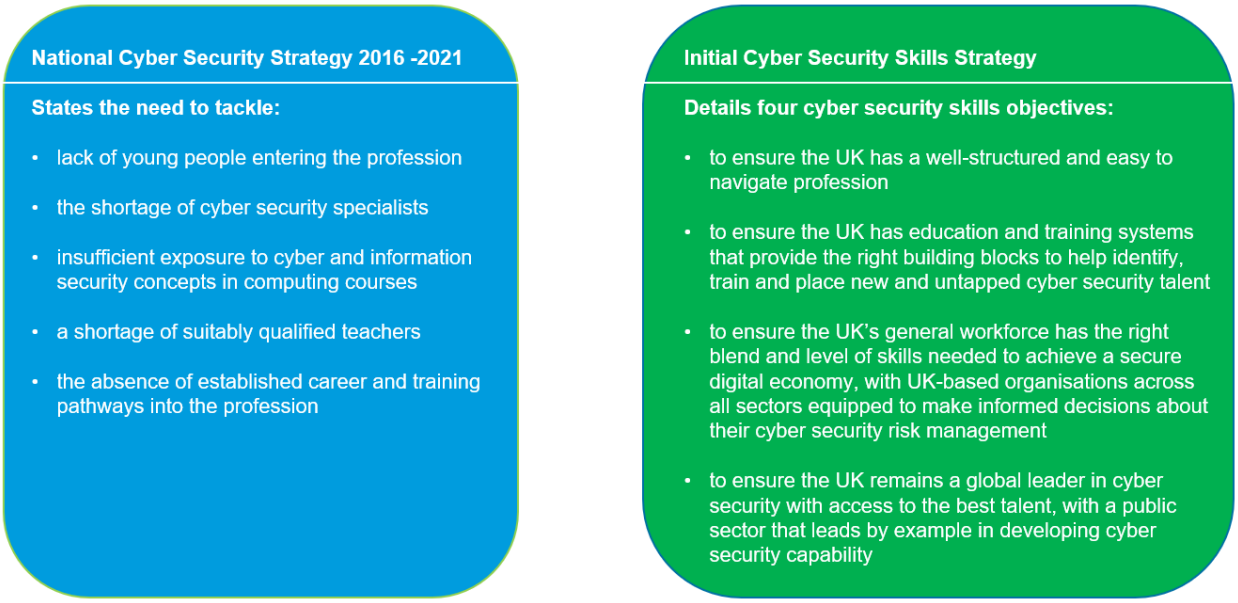
3. CONTEXT

3.1 Cyber Security Policy

The National Cyber Security Strategy 2016 to 2021[17] and Initial Cyber Security Skills Strategy[18] both highlight significant cyber security skills shortages in the UK. This is supported by recent research that suggests the skills gap in cyber security is growing significantly in the UK and across the world.

Figure 1 outlines the current UK cyber security policy priorities.

Figure 1 Cyber security policy priorities



3.2 Apprenticeship Policy

The UK 2020 'vision for apprenticeships' highlights the role of apprenticeships in skill development, productivity and economic growth. It includes a specific target to increase the quality and quantity of apprenticeships and to achieve 3 million apprenticeships by 2020.

In addition, the government has unveiled a review and consultation of level 4 and 5 qualifications, as it proposes that CertHE, DipHE and foundation degrees be rebadged as Higher Technical Qualifications (HTQs) and "quality approved" to attract more students to study them.

The Institute for Apprenticeships and Technical Education will work with employers through its Route Panels to approve qualifications, with a suggestion that non-approved level 4 and 5 provision will attract a lower fee cap and the removal of eligibility for teaching grant. The proposals suggest that the Office for Students (OfS) will be charged with developing an additional set of ongoing registration conditions specifically for higher technical providers. They include assessing suitably qualified and experienced teachers, links with employer networks and learning environments. Providers would be required to meet these new 'technical conditions' to be able to

[17] UK Government (2016) national cyber security strategy 2016 to 2021

[18] UK Government (2018) initial national cyber security skills strategy: increasing the UK's cyber security capability

deliver the approved HTQs, with access to relevant student finance and any additional public funding.

3.3 Business case for cohort 2

The National Cyber Security Programme 2 (NCSP2) year 1 business case for the programme states that newly trained cyber security professionals are needed to rapidly increase the availability of cyber security skills in the UK and contribute towards the objectives outlined in the (previous) UK Cyber Security Strategy. The strategy also highlights the need for competent, well-trained cyber professionals due to a significant and increasing mismatch in the supply and demand of adequately skilled cyber professionals.[19]

Companies consistently struggle to recruit adequately trained and certified staff and there is a significant risk that given a high proportion of the cyber workforce is coming towards retirement age, this skills gap will continue to grow. This is particularly concerning given that cyber breaches remain a tier 1 national security threat with the CNI and enabling sectors such as finance, energy and transport viewed as particularly vulnerable to attack.

The business case also included the following economic rationale[20]:

- if left on their own, individuals and firms fail to invest sufficiently in skills, justifying government support
- evidence shows there is a positive return for level 3[21] apprenticeships (the business cases notes there is limited data available for level 4 apprentices and therefore level 3 is used as the nearest proxy)

The NCSP year 2 business case also states that as the apprenticeship standards are new, there is a need to stimulate the market to prioritise cyber apprenticeships under the apprenticeship levy system and would require government help to do this.

3.4 Current need for cyber security resources

The 2018 Cyber Security Breaches Survey completed on behalf of DCMS found that in the previous 12 months, 43% of businesses and 19% of charities based in the UK experienced a cyber security breach or attack, while only 27% of businesses and 21% of charities in the UK have a formal cyber security policy.[22]

Overall prevalence of cyber security incidents

According to the Information Commissioners Office (ICO)[23] the number of reported cyber data breaches in the UK increased by over a fifth (21%) from 302 in the fiscal year 2016/17 to 364 in 2017/18.

Overall, cyber data breaches were most prevalent in financial organisations during this time period (increasing by 112.5% from 24 to 51 in 2017/18). However, transport experienced a higher relative

[19] UK Government (2011) UK cyber security strategy: protecting and promoting the UK in a digital world

[20] DCMS: NCSP2 year 1 Business Cases - Apprenticeships

[21] The business case noted limited level 4 data, hence level 3 data was used instead

[22] DCMS (2018) Cyber Security Breaches Survey

[23] https://ico.org.uk/action-weve-taken/data-security-incident-trends/ (accessed August 2019)

increase from 1 to 8 over the time period (+700%). The high baseline number of cyber breaches in financial organisations in 2016/17 indicates that the financial sector may be more exposed to cyberattacks than other CNI sectors.[24]

The following table outlines the number of cyber security incidents reported to the ICO by companies in CNI sectors. **Note – ICO classification can include a number of sectors; the following table maps CNI sectors to the ICO groupings however it is possible they include other sectors also. Those shaded in yellow relate to sectors involved in the cyber CNI apprenticeship programme (communications, transport and water). Due to the ICO classifications it was not possible to match some of the sectors that participated in the programme, e.g. energy and civil nuclear.**

Table 1: Data Security Incident Trends 2016/17 to 2017/18

ICO sector classification	CNI sector	Number of reported cyber breaches (2016/17)	Number of reported cyber breaches (2017/18)	Annual percentage change
Central Government	Emergency Services Defence Government	2	8	+300.0%
Charitable & Voluntary	No	24	26	+8.3%
Education	No	26	31	+19.2%
Finance, Insurance and Credit	Finance	24	51	+112.5%
General Business		74	110	+48.6%
Health	Health	58	37	-36.2%
Justice	No	3	4	+33.3%
Land or Property Services	No	4	10	+150%
Legal	No	7	21	+200%
Local Government	Emergency Services Government	12	5	-58.3%
Marketing	No	2	2	+0.0%
Media	Communications	6	5	-16.7%
Membership association	No	8	9	+12.5%
Online technology and telecoms	Communications	22	14	-36.4%
Political	No	1	2	+100.0%
Regulators	Government	3	2	-33.3%
Religious	No	2	1	-50%
Retail and Manufacture	No	12	4	-66.7%
Social Care	Health	2	1	-50.0%

[24] https://ico.org.uk/action-weve-taken/data-security-incident-trends/ (accessed August 2019)

ICO sector classification	CNI sector	Number of reported cyber breaches (2016/17)	Number of reported cyber breaches (2017/18)	Annual percentage change
Transport and Leisure	Transport	1	8	+700.0%
Utilities	Water	2	4	+100.0%
Other		7	7	+0.0%
Total		302	364	+21%

A recent report[25] found the UK cyber security labour market is relatively immature, with only a small number of individuals having previously worked in professional roles in cyber security and some may have absorbed this role into an existing non-cyber security job. Moreover, it is suggested that there is a large informal cyber security sector, where the individuals working in these roles often lack the technical expertise, skills or experience to fully understand or carry out their work.[26]

The growing number of cyber security attacks combined with the concern regarding lack of professional skills, highlights the need for government intervention.

3.5 Cyber security apprentices

Research on the UK cyber security skills market[27] found that the prevalence of cyber apprenticeships across the private, public and charitable sectors is relatively low. However, findings from interviews with external cyber security providers indicated apprenticeships are a common recruitment method and cyber or IT apprenticeships can be a career path into the industry.

The research also noted it can be a challenge for smaller companies to offer apprenticeships, given the lack of relevant cyber security skills and time from existing team members to train and supervise apprentices.[28] As a result they tend to recruit staff with pre-existing technical skills.

It is also suggested that the types of apprenticeships differ between external cyber security providers and other organisations. While some external providers prefer cyber apprenticeships to allow a deeper understanding of this specialist area, IT apprenticeships are common among other organisations "reflecting that cyber security was often managed as part of a wider IT role".

There is general evidence[29] that employers and prospective learners are increasingly valuing apprenticeships as a channel of recruitment and a viable career pathway. Recent research[30] found that almost four fifths (77%) of young people surveyed (n=1,000) believed that apprenticeships

[25] Ipsos Mori (2018) Understanding the UK Cyber Security Skills Labour Market

[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] Ipsos Mori (2018) Understanding the UK Cyber Security Skills Labour Market

[28] The report notes this was more of a problem for cyber apprenticeships than for general IT apprenticeships, where existing staff were more likely to have relevant skills and knowledge to impart.

[29] Grant Thornton (March 2018) Generation Apprentices – The Evolution of Earn as you Learn

[30] Grant Thornton (March 2018) Generation Apprentices – The Evolution of Earn as you Learn

offer good career prospects. Similarly, in a survey of 500 levy-paying employers, 86% of employers surveyed had apprentices currently employed in their business and 50% intended to recruit more than they currently do within the next 5 years. In relation to why employers value apprenticeships 51% noted that apprenticeships afforded the ability to develop and train people to meet specific business needs, 50% noted that they brought in new ideas and innovation and 86% of employers felt that apprenticeships increased social mobility within their organisation.

Moreover, research[31] on identifying the role of further and higher education in cyber security skills found that entry-level jobs in cyber security usually involve less specialisation, with graduates spending 2 to 3 years undertaking a variety of IT roles before moving, perhaps after receiving in-house training, into a cyber security role. However, it is also highlighted that the situation differs in smaller organisations which typically recruit graduates with general qualifications however do not have the capacity or scale to allow a high degree of specialisation, whether in cyber security or any other IT.[32]

3.6 Cyber security apprenticeship standards

Apprenticeship standards were introduced in response to the 2012 Richard Review of Apprenticeships[33], which stated that apprenticeship outcomes should be "meaningful and relevant for employers". Standards are developed by trailblazer groups that represent groups of employers and sector organisations and include an end-point assessment. The first standards were introduced in September 2014.[34]

There are five apprenticeship standards that contain some elements of learning in cyber security: two at level 4; two at level 6; and one at level 7. In these two standards, cyber security is effectively a specialism in a broader education programme. This evaluation has considered if the focus on level 4 reflects the needs of companies in the CNI sector.

Both level 4 standards were reviewed by the Institute for Apprenticeships in 2019[35] which concluded that the Cyber Intrusion Analyst (Level 4) will be withdrawn and incorporated into the Cyber Security Technologist standard (Level 4).[36]

The Level 6 and Level 7 apprenticeships typically offer a broader education in cyber security and digital and technology solutions. The level 7 apprenticeship focuses on the managerial and strategic aspects of digital solutions and cyber security.

Figure 2 provides an overview of the cyber security apprenticeship standards, including those with a cyber security element.

[31] Centre for Strategy and Evaluation Services (2018) Identifying the Role of Further and Higher Education in Cyber Security Skills Development

[32] Centre for Strategy and Evaluation Services (2018) Identifying the Role of Further and Higher Education in Cyber Security Skills Development

[33] Richard, Doug (2012) The Richard Review of Apprenticeships

[34] Powell, Andrew (2019) Apprenticeships and skills policy in England

[35] Institute for Apprenticeships and Technical Education (2019) statutory review report: digital route

[36] The Institute has reviewed the evidence from the public consultation, trailblazer group engagement, expert peer review feedback, performance data, analysis against the Institute's quality criteria and the expertise of the Route Panel. This ascertained whether the apprenticeship standards in scope were underpinned by genuine occupations, in demand from employers, and appropriate for an apprenticeship

Figure 2: Overview of cyber security apprenticeship standards

Digital and Technology Solutions Specialist Degree Apprenticeship (Level 7) – This standard focuses on the strategic elements of digital and technological solutions including the review and improvement of complex IT enabled business processes, the design of technology roadmaps and implementation strategies and delivery of technology-based business change programmes. The standard is primarily focused towards the higher managerial aspects of organisational digital and technology and prepares apprentices to operate effectively with higher organisational management and successfully manage strategic processes at the expense of less detailed and intensive instruction in cyber security related areas.

The expected length of the standard is around 18 months and employers will set entry requirements but are likely to include a 2:1 degree or higher in a relevant subject.

Cyber Security Technical Professional Degree Apprenticeship (Level 6) – This standard provides a broader digital and cyber education but somewhat less specialised cyber expertise such as a forensic specialist. Business skills are developed with the potential to work autonomously and lead a team however with less impact on the business's IT structure. The standard should enable apprentices to design and build complex and simple networks, systems and algorithms all while fitting and conforming to the requirements of an organisation. Apprentices under this standard should, upon completion, also be able to undertake risk modelling, analysis and trades as well as performing a variety of organisational functions in relation to cyber security including developing information management plans and assurance strategies.

While individual employers will set the selection criteria the starting point is likely to include three 'A' levels, including maths, or other relevant qualifications or experience.

Digital and Technology Solutions Professional Degree Apprenticeship (Level 6) – This standard provides a broad education in digital technology solutions including cyber security, business and system analysis, data analysis and network infrastructure. The standard has a core technical knowledge focus on the impact of digital solutions on business, including how they can be exploited for competitive advantage, the value of digital business investment and the role of data management systems in protecting organisational data. Although the standard provides a general higher-level education in all of the aforementioned digital strands, students have the opportunity to specialise in one of the core subject areas of the standard. Consequently, the intensity and volume of cyber security instruction and knowledge in this apprenticeship is largely down to the specialisation decisions of the apprentice.
The standard typically takes at least three years and while individual employers will set entry requirements these may include A-levels including maths or other relevant experience or qualifications.

Cyber Security Technologist (Level 4) - The Cyber Security Technologist standard teaches candidates to analyse and identify flaws in cyber security infrastructure and to analyse, evaluate and respond to security threats and hazards. Through the apprenticeship candidates will gain an awareness of common attack types and appropriate responses as well as being able to conduct risk assessments of simple systems. The standard comprises of two specialisation tracks, technologist and risk analyst. The technologist track focuses on the design, maintenance and troubleshooting of networks as well as analysis of organisational security requirements and structured and informed implementation of security to organisational networks. The risk analyst track focuses on cyber security procedure including conducting risk assessments, audit and assurance, incident response and establishment and promotion of an organisational cyber security culture.
Individual employers will set selection criteria, but these are likely to include A-levels, a relevant level 3 apprenticeship or other relevant qualifications.

Cyber Intrusion Analyst (Level 4) – The Cyber Intrusion Analyst standard focuses on the identification of anomalies and breaches in network security to feed into organisational incident response. The standard teaches apprentices to integrate and analyse information from a wide range of sources and to monitor network systems for signs of breaches using a variety of automated tools. Apprentices in the standard will gain experience of accurately recording incidents and writing subsequent reports as well as undertaking root cause analysis of potential breaches and suggesting improvements to monitoring systems to reduce inaccuracy. Candidates will also be able to undertake research to identify threats and hazards and manage local responses to non-major incidents.
The expected duration of the apprenticeship is two years and individual employers will set recruitment standards that are likely to include A-levels, a Level 3 apprenticeship in a relevant area or other relevant qualifications.

The level 4 cyber security apprenticeship standard (comprising the options of Cyber Security Technologist and Intrusion Analyst[37]) was created in 2016 based on support from those involved in the trailblazer group.[38]

Consultee feedback highlights the apprenticeship was designed to pioneer new routes into the profession that could potentially lead onto graduate level. However, the route to achieve this is not clear since the level 4 standard does not cover everything in the first stage of the level 6 digital technology solutions professional standard. The lack of coordination between apprenticeship standards means that pathways for apprentices are not clear. In addition, qualitative feedback from consultees suggested that many employers are struggling to understand what skills or resources they need or how these relate to the apprenticeship levels noted above.

3.7 Uptake of apprenticeships

3.7.1 Generally

Data from the Department for Education (DfE)[39] states that the total number of apprenticeship enrolments in apprenticeships (from Level 3 to 7) fell between 2017/18 and 2018/19 by 8.4%. This follows a similar period of contraction between 2016/17 and 2017/18. However, this is mostly due to a decline in the uptake of level 3 qualifications, which account for most enrolments and declined by almost a fifth (17.8%) from 2017/18 to 2018/19.

However, levels 4 and Level 5 uptake increased significantly, with enrolments in level 4 qualifications almost doubling from 2015/16 to 2018/19. In addition, the number of higher-level apprenticeships has increased with level 6 apprenticeship uptake more than doubling between 2015/16 and 2016/17 (from 740 to 1,650) and thereafter increasing to 6,370 in 2017/18. Level 7 also more than doubled between 2017/18 and 2018/19 Q3 (from 4,500 to 9,690). The high-level trends suggest that while aggregate demand for apprenticeships has fallen in recent periods, there has been a marked shift towards increased demand for higher level apprenticeships.

The following table shows the average annualised growth in uptake of apprenticeships in specific CNI sectors across all relevant qualification levels (i.e. 3 to 7).

[37] Institute for Apprenticeships and Technical Education (2019) statutory review report: digital route. Both standards were reviewed by the Institute for Apprenticeships in 2019 which concluded that the Cyber Intrusion Analyst (Level 4) will be withdrawn and incorporated into the Cyber Security Technologist standard (Level 4)

[38] Trailblazer groups are responsible for developing new apprenticeship standards and are expected to employ apprentices in the occupation once it is developed and to market the apprenticeship standard actively once it is approved for delivery

[39] Department for Education: Apprenticeship and Levy Statistics December 2018 (2015/16 – 2017/18)

Table 2: Annualised growth in uptake of apprenticeships in specific CNI sectors 2015/16 - 2018/19 (Q3)

CNI Sector	Average Annualised Growth in Apprenticeship Uptake (2015/16 - Q3 2018/19)
Emergency Services	516%
Government	267%
Transport	207%
Communications	180%
Finance	128%
Food	117%
Civil Nuclear	93%
Defence	82%
Water	52%
Energy	39%
Health	35%

Source: Department for Education: Apprenticeship and Levy Statistics December 2018 (2015/16 – 2017/18).
Note – data is rounded to the nearest 10

All CNI sectors on average recorded an increase in apprenticeship uptake from 2015/16 to 2018/19. The emergency services, government and transport sectors recorded the largest average proportional increase; however these sectors had a relatively low baseline uptake. The communications sector (of which cyber security apprenticeships are a constituent standard) recorded strong growth in uptake across levels 3 to 7, increasing by 180.1%.

3.7.2 Apprenticeships in cyber security

The number of apprenticeships starts per standard (i.e. uptake) is outlined in the following table (the first three are focused on cyber security while the last 2 have cyber security elements).

Table 3: Number of apprenticeships starts per standard 2015/16 to 2018/19 (Q3)

Standard	Level	Approval Date[40]	Uptake 2015/16	Uptake 2016/17	Uptake 2017/18	Uptake 2018/19 (Q3)
Cyber Intrusion Analyst	4	23/03/16	0	10	10	10
Cyber Security technologist	4	10/05/16	0	100	240	250
Cyber Security Technical Professional	6	24/09/18	0	0	0	20
Digital and Technology Solutions Professional Degree[41]	6	26/03/15	350	520	1,310	1,400
Digital and Technical Solutions Specialist	7	07/08/18	0	0	0	130

Source: Department for Education: Apprenticeship and Levy Statistics December 2018 (2015/16 – 2017/18).
Note – data is rounded to the nearest 10

[40] Relates to the date the standard was approved and the first year it would have been able to run, however it may have taken further time for training to begin

[41] There is a standard Cyber Security Specialist that is a specialism within the level 6 DTS standard https://www.instituteforapprenticeships.org/apprenticeship-standards/digital-and-technology-solutions-professional-integrated-degree/ (accessed August 2019)

The Cyber Security Technologist apprenticeship has increased year on year from 100 in 2016/17 to 240 in 2017/18 and 250 in 2018/19 (Q3). This compares favourably to the level 4 Cyber Intrusion Analyst standard which has seen uptake remain low and static over the last few years. However, it should be noted that not all courses were being delivered for all of time periods in table 3, and therefore '0' uptake does not necessarily mean zero interest.

Due to the way information is collected for the level 6 Digital and Technological Solutions standard it is not clear how many individuals take cyber security options within this track.[42] Moreover, it is too early to measure take up against the Cyber Security Technical Professional (Integrated Degree) standard at level 6 as this is still quite new to the market.

IT related standards that are comparable to cyber security apprenticeships (in terms of level, baseline uptake and approval date) include the Data Analyst standard and the IS Business Analyst (both subjects are specialisms within the Digital and Technical Solutions Specialist apprenticeship). **Both have experienced a significantly faster average growth in uptake than either of the level cyber security standards[43]:**

- Data Analyst standard – uptake increased from 60 in 2016/17 to 1,420 in 2018/19
- IS Business Analyst standard – uptake increased from 10 in 2016/17 to 370 in 2018/19

The Data Analyst apprenticeship has a significantly higher uptake and average growth than either level 4 cyber security apprenticeship.

The available evidence indicates an increase in interest in cyber security related qualifications over the last few years, however while the standards are relatively new, the need to rapidly increase cyber security skills is not being delivered to the extent it should.

3.8 Conclusion

It is too early to conclude on the full extent to which the cyber CNI apprenticeship level 4 programme has contributed to policy objectives in relation to building the UK"s cyber security knowledge, skills and capability and increasing the availability of cyber security skills.

However, a key purpose of the programme was to stimulate the market to prioritise cyber apprenticeships, this was not achieved as the uptake was low. Later sections consider the reasons for this and make recommendations.

[42] There is a standard Cyber Security Specialist that is a specialism within the level 6 DTS standard. https://www.instituteforapprenticeships.org/apprenticeship-standards/digital-and-technology-solutions-professional-integrated-degree/ (accessed August 2019)

[43] Department for Education: Apprenticeship and Levy Statistics December 2018 (2015/16 – 2017/18)

4. STATE OF THE SECTOR

4.1 Embryonic state of cyber security

A Cybersecurity Capacity Review of the United Kingdom[44] notes that cybersecurity maturity in the UK remains embryonic. While there are a number of initiatives such as the Cyber Discovery[45], the CyberFirst Bursary[46], CyberFirst Degree Apprenticeships[47], the Cyber Security Immediate Impact Fund (CSIIF)[48] and cyber bursaries programme[49] as well as the establishment of the National Cyber Security Centre (NCSC), **there remains a lack of detailed understanding of systemic cyber risk.**

Research[50] on the UK cyber security skills labour market found that private sector businesses and charities often do not fully understand the technical skills cyber security jobs require.

Qualitative feedback from key stakeholder consultees (professional bodies, representative bodies and those in the FE sector) who have completed consultation and engagement with CNI and non-CNI companies suggest that many remain unaware of cyber security risks and therefore the skills needed to address these.

> "the market is not valuing, and therefore not managing, cyber risk correctly [and] cyber risk is still not fully understood and managed across much of the CNI, even as the threat continues to diversify and increase"
>
> Third Report of the Joint Committee on the national security strategy (November 2018) cyber security of the UK's critical national infrastructure

4.2 Lack of evidence as to what levels are needed

It is difficult to determine what type of government intervention is needed to support the CNI sector with cyber security skills for several reasons.

First, there is a lack of evidence on what level of cyber security skills are required by companies, what the gaps are, and what resources needed to fill these in the CNI sector.

A recent report[51] found that basic technical skills[52] gaps are more evident in the food or hospitality, construction, retail or wholesale and professional scientific or technical firms. Meanwhile, high level

[44] Global Security Capacity Centre (2016) Cybersecurity Capacity Review of the United Kingdom

[45] Initiative aims to help plug the UK's cyber security skills gap by tapping into young and undiscovered talent with the ambition of stimulating and nurturing interest in cyber security as a future career path

[46] CyberFirst is a student scheme inspired and led by the National Cyber Security Centre (NCSC) which aims to support and prepare undergraduates for a career in cyber security. NCSC partners with other government departments and selected industry, offer students £4,000 per year and paid cyber skills training to help start a career in cyber security.

[47] The CyberFirst Degree Level Apprenticeship is a three year apprenticeship which provides applicants a starting salary of £18,495 and opportunity to gain a recognised degree over the three-year programme.

[48] Aims to increase the diversity and numbers of those working in the UK cyber security sector.

[49] Offered bursaries to adults transitioning into a career in cyber security by taking a GCHQ-certified master's courses.

[50] Ipsos Mori (2018) Understanding the UK Cyber Security Skills Labour Market

[51] Ipsos Mori (2018) Understanding the UK Cyber Security Skills Labour Market

[52] Basic technical skills are defined as those which are needed to implement the minimum technical controls laid out in the government-endorsed Cyber Essentials scheme. This includes: secure internet connections, secure devices and

technical skills[53] gaps are more prevalent in entertainment, service or membership organisations[54], utilities or production, information or communication and construction firms. However, it may be reasonable to expect that companies who stated they were missing basic technical skills are also missing high level technical skills and it is possible that companies may not understand the differences between basic and high level skills.

The report[55] also estimates that:

- of the approximately 1.32 million businesses in the UK, approximately 710,000 have a basic technical cyber security skills gap
- of the c.199,000 registered charities, approximately 107,000 have this gap
- of the c.12,400 public sector organisations, approximately 2,200 have this gap

Secondly, the cyber security environment is continuously changing due to advancements in technology and the rapidly changing threat landscape resulting from the growing use of mobile technology, IoT, cloud computing and data centres. The profession continues to be embryonic and therefore companies are unclear what resources they need to deploy to minimise cyber risks.

4.3 Different levels of cyber security awareness and maturity in the CNI sub sectors

The UK cyber security labour market is relatively immature and as a result there is no published data on the size of the cyber security skills gap linked to educational levels or specific job roles.

Many companies are unsure of what skills they need, at what level and what capabilities are required within their organisation, with some staff absorbing a cyber security role into an existing non-cyber security job.[56] This has resulted in an informal cyber security sector, where individuals working in these roles often lack the technical expertise, skills or experience to fully understand or carry out their work.[57]

software, controlling user access to data and devices, protection from viruses and other malware, and keeping devices and software up-to-date

[53] High level technical skills include the following broad high-level technical skills areas: security architecture, penetration testing, threat intelligence, forensic analysis, interpreting malicious code, and user monitoring

[54] While entertainment, service or membership organisations come have the highest % that are not confident in carrying out one or more of the 6 high level tasks, it is worth noting the very small sample size for this particular sector. This means that the margins of error around the survey findings for this sector are especially high, and this finding should be treated with caution

[55] Ipsos Mori (2018) Understanding the UK Cyber Security Skills Labour Market

[56] Ipsos Mori (2018) Understanding the UK Cyber Security Skills Labour Market

[57] Ipsos Mori (2018) Understanding the UK Cyber Security Skills Labour Market. An important caveat for these findings is that they do not specifically reflect firms in the cyber security industry itself (i.e. working on cyber security technological developments, products or services) – they represent those working in cyber security roles within other industries

The second report[58] by the Joint Committee on the national security strategy on cyber security skills and the UK's critical national infrastructure suggests a significant gap between the demand and supply of skills in relation to higher level skills, in particular:

- the elite, highly specialist skills and knowledge required by the relatively small numbers of employees whose principal task or research area is the security of a given system, network or device against cyber threats, for example a network architect or penetration tester
- the moderately specialist skills and knowledge required by all those whose jobs have now assumed an important cyber security element, for example teachers, lawyers, auditors, HR managers or board level directors who need to understand the cyber risk to business operations

It is suggested that the gap between demand and supply is exacerbated by government and industry often looking for employees from the same 'pool' of talent, which is restricted further by the requirement that some CNI sector employees need to have a certain level of security clearance.

Some smaller companies face further difficulties in offering apprenticeships as they may lack the relevant cyber security skills and time from existing team members to train and supervise apprentices.[59] As a result they try to recruit staff with pre-existing technical skills.

A recent report[60] by the Federation of Small Businesses (FSB) found that SMEs are critical to achieving the government's target of reaching 3 million new apprenticeships by 2020, however some smaller companies often lack the relevant cyber security skills and resources to recruit, train and supervise apprentices.[61] As a result they try to recruit staff with pre-existing technical skills.

Consultation feedback from one professional body and SME consultees (n=2) also highlighted that SMEs may not be considering cyber security apprenticeships due to:

- resource / expertise needed: most do not have the support infrastructure they would need to put in place (the DCMS cyber CNI apprenticeship programme required each participating company to have a line manager and mentor for apprentices). While this is possible in larger organisations with an IT / cyber department and an apprenticeship infrastructure, it may not be feasible in smaller organisations which may only have 3 IT or cyber staff members. In addition, 2 SME consultees highlighted smaller companies may not be able to provide apprentices with sufficient breadth of experience to support the completion of their portfolio or the management time required to help them develop skills for everyday work (for example, time keeping as well as report writing, problem solving and interpersonal skills)
- financial cost: SMEs do not have the funding they would need to invest (e.g. to cover the apprentice and line manager time). One SME consultee also highlighted that the apprentice training time required could have an impact on the wider team if there were only a small number of cyber security staff working on a project

[58] Joint Committee on the national security strategy (July 2018) Cyber Security of the UK's Critical National Infrastructure

[59] The report notes this was more of a problem for cyber apprenticeships than for general IT apprenticeships, where existing staff were more likely to have relevant skills and knowledge to impart

[60] Fit for the Future (2019) Making the Apprenticeship System Work for Small Businesses

[61] The report notes this was more of a problem for cyber apprenticeships than for general IT apprenticeships, where existing staff were more likely to have relevant skills and knowledge to impart

- lack of information / knowledge: SMEs may not know skills they need, or the interventions available to address these

To overcome the challenges SMEs face in engaging with apprenticeships a recent report by the all-party parliamentary group (APPG)[62] on apprenticeships recommended that[63]:

- the government should encourage levy-paying businesses to use the 10% of their funds to be shared with SMEs in their supply chain or in their local community
- Local Enterprise Partnerships (LEPs) should act as a forum to introduce SMEs to bigger employers and providers in a safe and supporting environment and be constantly promoting the positive messages on hiring apprenticeships to SMEs in their local area
- organisations that work with SMEs daily, for example banks, accounts and HMRC should promote apprenticeships to their SME customers and consider how they can help SMEs to recruit apprentices
- MPs should consider using the APPG's Apprenticeship Fair Toolkit for MPs to organise apprenticeship fairs in their constituency at least annually and encourage SMEs to take an active part
- more training on the apprenticeships levy should be offered to HR professionals in businesses of all sizes and to procurement officers to enable an increased understanding of how they can use apprenticeships to maximum effect
- big employers should appoint a board-level champion for apprenticeships within their organisation, with a specific remit to consider how their business can support SMEs in their supply chain, sector or local area to hire more apprentices
- pilots should be set up to pool apprenticeship levy underspend, which would be accessed by councils or combined authorities with the purpose of supporting SMEs recruit more apprentices. This should include establishing a Small Business Service supported by the LEP and larger businesses based in the region

Given the importance of the CNI sector to the rest of the economy and society it is important that employers are provided with supports, such as those outlined above, to help overcome any barriers to engaging with apprenticeships.

4.4 Lack of information on how skills and expertise relate to the cyber security apprenticeship levels

It is not possible to accurately link apprenticeship levels to the basic or high-level skills identified in recent research.[64] In addition, cyber security apprenticeships were and continue to be a relatively immature route into the profession, with DfE statistics[65] showing there were 590 cyber security technologist apprentice starts in the period 2016/17 to 2018/19. While data is held on the

[62] All-Party Parliamentary Groups are informal groups of members of both Houses with a common interest in particular issues

[63] All party parliamentary group on apprenticeships (2018) Toolkit: helping SMEs hire more apprentices

[64] Ipsos Mori (2018) Understanding the UK Cyber Security Skills Labour Market

[65] Apprenticeship framework/standard demographic and sector subject area; Pivot Table Tool: starts and achievements 2014 to 2015 to Q3 2018 to 2019 (accessed July 2019)

companies using the standards by the Institute for Apprenticeships and Technical Education , they were unable to share this information and therefore it is not known how many companies in the CNI sector have cyber security apprentices.

4.5 Conclusion

The cyber security skills requested by companies vary depending on awareness of cyber security risks; awareness of cyber security skills or roles and willingness to invest in an appropriate resource / support for their need.

There is a lack of detailed evidence on what cyber security skills are needed by companies in the CNI sector. The information that exists focuses on basic and high level skills, however this is not linked directly to the apprenticeship standards. There is also evidence that some companies are not clear on how to assess their cyber security skill needs or how best to fill these.

5. PERFORMANCE OF COHORTS 1 AND 2

This section outlines performance and key findings from the apprentice and employer surveys / consultations as well as feedback from sector stakeholders and output information provided by QA against the evaluation research questions.

5.1 Programme description

The cyber CNI apprenticeship programme delivered the level 4 Cyber Security Technologist standard which focuses on the areas of:

- understanding of cyber threats, hazards, risks, controls and remediation measures
- mitigations to protect organisations systems and people

The programme involves 57 days of classroom training supported by digital content and activities through the virtual learning platform.[66] During the programme the apprentices are required to spend 20% of their time on off the job training.[67] The programme is made up of the following 4 components[68]:

- **knowledge modules** - combination of classroom workshops at a local QA Apprenticeships learning centre and online learning. Each classroom workshop typically takes place in a one week block. At the end of some modules, apprentices complete an assessment in the classroom. Online learning supports the face to face learning, before and after the classroom workshops. It can be completed in the workplace to fit around their job. These classroom assessments must be passed before the end point assessment can take place
- **portfolio** – showcases real work projects to demonstrate the skills and behaviours learnt and practically applied in the workplace while on the programme to ensure they have the required skills set out in the apprenticeship standard. It is designed to show how the apprentice has applied their learning in a holistic and coherent way appropriate to their role in the workplace. It is presented towards the end of the apprenticeship and is assessed as part of the end point assessment
- **synoptic project** - a holistic assessment during which the apprentice applies skills to solve a business-related problem. The project takes place in the classroom in a controlled assessment environment
- **end point assessment interview** - carried out by BCS, the Chartered Institute for IT, covering the project and contents of the portfolio. The interview assesses whether the apprentice has successfully met the learning requirements of the programme and decides whether successful apprentices are awarded a pass, merit or distinction.

In addition, the participating employer is expected to provide a reference which outlines their perspective on how the apprentice has performed in the workplace and how they have applied

[66] This delivery model was created by QA

[67] Refers to training during the programme takes place in the classroom environment at a QA Centre and done in the workplace, through online training, workplace assessments, developmental activities set by the Skills Coach, or developing their portfolio

[68] QA (2018) Cyber Security Technologist Level 4

their knowledge, competencies and behaviours in work projects. It is also used to verify and support evidence of capability submitted in the summative portfolio. An apprentice who successfully completes the apprenticeship is eligible to apply for Associate Membership of the IISP and BCS and for entry onto the Register of IT Technicians (RITTech).

5.2 Performance

The following table details the number of apprentices enrolled across both cohorts and in total. Overall the original target (150 apprentices) and revised target (75 apprentices) has not been met.

Table 4: Number of cohort two apprentices who completed the programme

Cohort	Total enrolled	Withdrew	Number who have completed their end point assessment	Number who have passed	Pass rate[69]
Cohort 1	19	4	9[70]	9	100%[71]
Cohort 2	32	3[72]	12[73]	12	100%[74]
Total	51	7	21	21	100%

Source: Information provided by QA to RSM (September 2019)

It is not possible to state of those that have completed the end point assessment how many have confirmed jobs as not all employers and apprentices chose to take part in the evaluation. However, the 11 employers consulted stated that 22 of their 23 apprentices will remain in a cyber security role in their organisation, indicating an employment rate of 95.7%. If this rate is applied to the 44 apprentices who are expected to complete the programme, it results in a **projected 42 gross jobs**.

[69] Number who have passed divided by the number who have completed the end point assessment to date

[70] 3 x Distinction; 2 x Merit; and 4 x Pass

[71] The remaining 10 apprentices are going through the End Point Assessment process. Some of these had previously completed the End Point Assessment however were unsuccessful and are resubmitting

[72] One further apprentice chose to complete the programme with another training provider

[73] 5 x Distinction; 1 x Merit; 6 x Pass

[74] Of the remaining 20 apprentices, 9 are currently going through End Point Assessment process and 11 are still on the programme

5.3 Key findings

The following key findings are based on evidence collected from interviews and surveys with apprentices and employers participating in the programme, companies who did not participate in the programme and strategic stakeholders in the sector. The findings in this section are based on feedback from:

- survey of apprentices (n=19)
- interviews with CNI employers who participated in the programme (n=9) and two who completed the CNI employer survey
- the non-participating employer survey (n=14) (companies who were contacted by DCMS to participate in the programme however declined to do so at that stage)
- strategic stakeholder interviews (n=34)

Table 5: Research questions and key findings

Research question	Key findings
What are the key lessons that can be learnt regarding the structure of the scheme?	The programme was run as a closed cohort which meant apprentices were in sessions only with others on the DCMS cyber CNI apprenticeship and were not interacting with apprentices on other QA apprenticeship programmes. There were mixed views on the structure of the programme. While some companies valued the closed cohort approach to help develop peer relationships between apprentices and with other companies; some employers and QA suggested an open cohort would allow for greater exchange of experience and ideas between sectors. **Feedback from companies on what worked well and areas for development includes:** Worked well: 1. 20% mandated time for off the job training as this allowed dedicated time for learning and the process of repeated, periodic learning and application was useful 2. information on what modules the apprentices would take which provided an understanding of apprentices were learning Areas for development: 1. greater support from the Skills Coaches, suggesting they were not able to dedicate the time needed to support apprentices 2. inclusion of more analyst orientated modules in the training 3. content and provision could be improved by moving away from descriptive content and teaching guidelines 4. better monitoring of the training provider's performance by DCMS

Research question	Key findings
	Feedback from apprentices on what worked well and areas for development includes: Worked well: 1. training modules and timing of training 2. support from the employer 3. getting industry experience 4. networking with other industry professionals Areas for development: 1. support from the Skills Coaches, in relation to technical knowledge and being more accessible to answer questions and queries 2. communication from QA, including more clarity on the work required and better information on how the apprenticeship will 'map out' at the start 3. provision of other, less technical, modules and less focus on
Apprenticeship numbers including dropout rates, number of applicants per post, the pass rate	There were a significant number of eligible apprentice applicants for both cohorts (1,024 in cohort 1 and 1,164 in cohort 2), resulting in 51 apprenticeships in total. Therefore, the current processes appear effective. This suggests an overall conversion rate of 3% however due to the lower than anticipated number of employers there were a limited number of apprenticeships available and as a result the original target of 150 new apprentice starts was not met. Consultation with the recruitment provider indicated that at the assessment suite stage Capp selected the top 20% - 30% of respondents. Current data for cohort 1 indicates a pass rate of 67% with 3 end point assessments still to be completed. Overall there were 7 dropouts (14%) which is similar to other cyber security apprenticeship programmes. For example, in the 2016 intake for the Government Security Profession Unit (GSPU) cyber security programme (also delivered by QA), there were 19 starts and of these 3 dropped out (16%, one moved to another government job, one to the private sector, and one to GCHQ).
The type of standard, popularity, and roll out (including geographic location, age etc) **Why was the scheme primarily the Cyber Security Technologist?** **Why was the focus on Level 4 not 6?** **Any difference in the popularity of standards/levels and any suggestion as to future focus on**	The level 4 Cyber Security Technologist, along with the Cyber Intrusion Analyst, was one of 2 pathways available at level 4. The cyber CNI apprenticeship programme focused on Cyber Security Technologist as the Cyber Intrusion Analyst programme had not been approved[75] by BCS Ofqual for delivery when the programme commenced. There is no documented, robust rationale for choosing the level 4 Cyber Security Technologist standard. Feedback from DCMS consultees indicated the business case was linked to policy objectives focused on developing cyber security talent generally. All apprentices on the programme undertook the Cyber Security Technologist standard however as a number of employers had

[75] While it was initially anticipated that the programme would offer both the Cyber Security Technologist and Cyber Intrusion Analyst, the knowledge modules and exams were not developed when cohort 1 and cohort 2 commenced

Research question	Key findings
these standards or flaws in these current standards?	expressed a preference for the analyst standard DCMS funded additional training that mapped across to some of the areas on the Intrusion Analyst standard However, companies suggested that the programme focused too much on the technologist aspect (e.g. on building networks) and insufficient learning on the skills required for an analyst role (e.g. report writing skills). This may be addressed by the recent IFATE recommendation that that the Cyber Intrusion Analyst (Level 4) will be withdrawn and incorporated into the Cyber Security Technologist standard (Level 4). [76] It is too early to measure take up against the Cyber Security Technical Professional (Integrated Degree) standard at level 6 as this is still quite new to the market.
The types of employers, amount, locations and sectors in CNI. **How were employers recruited?** **Could there have been a better way?** **What were the reasons behind the uptake in numbers?** **Did the scheme try to expand to other CNI sectors?** **Do CNI employers face any additional barriers in taking part in the scheme?**	The marketing of the programme to employers was limited to a ministerial letter[77] to companies in the CNI sectors alongside DCMS using their existing contacts with CNI employers and via working groups. This was initially focused on energy, transport and defence and was expanded to include more sectors[78] for cohort 2. This approach was resource intensive and an interim evaluation of the programme highlighted that more dedicated resources were needed to deliver a 'a more meaningful engagement campaign [with] sustained outreach effort and follow up'. Uptake from companies may have been impacted by: • timing – cohort 1 companies suggested this was out of sync with their normal recruitment process. This normally occurs in September with a start date one year later, however recruitment for the cyber CNI apprenticeship programme was undertaken in January 2017 and the apprentices started in April of the same year • awareness of cyber security skills needs - research suggests that some companies are either not aware of their cyber security needs or are not prioritising cyber security • the marketing of the programme - needs to be more extensive, ensuring that many more companies are informed of the programme, while also being given information on cyber security risks and the ways in which these cyber security apprentices can help companies. Case studies from the pilot programme could be used to help inform employers of the benefits CNI employers did not offer any evidence of additional barriers they faced compared with non CNI employers. While data is held on the companies using the standards by the Institute for Apprenticeships and Technical Education they were

[76] Both standards were reviewed by the Institute for Apprenticeships in 2019 which concluded that the Cyber Intrusion Analyst (Level 4) will be withdrawn and incorporated into the Cyber Security Technologist standard (Level 4). Institute for Apprenticeships and Technical Education (2019) statutory review report: digital route

[77] 40 companies were initially contacted in autumn 2016 and an additional 100 were written to via a ministerial letter in 2017

[78] Expanded to include water, telecoms, cyber and media

Research question	Key findings
	unable to share this information and therefore it is not known how many companies in the CNI sector have cyber security apprentices.
The reach and success of marketing **How were the existing channels utilised?**	Apprentices were recruited by QA and Capp using several methods, including[79]: • online – for example QA website and job boards • direct engagement – for example newsletters and e-shots • influencer engagement – for example youth liaison officers • social media – for example Facebook, Twitter and Instagram Most applicants heard about the programme via Indeed, the National Apprenticeship Service (NAS), the CV library and 'Get my first job'.
The quality of the recruitment **How difficult was it to find good quality students?** **What was the impact of the selection criteria on student uptake?** **What did employers consider as to the quality of students?**	There were a significant number of applicants for both cohorts that met the eligibility criteria (1,024 in cohort 1 and 1,164 in cohort 2). Feedback from the training provider suggested they normally have fewer applicants however it was agreed with DCMS to widen the A-level criteria to include any A level and not only STEM. Both the recruitment provider and participating companies suggested overall the quality of applicants was good, with all companies (that provided feedback) obtaining the number of apprentices they required. As the number of applicants was high, therefore it is clear these routes were effective. Given the small numbers of companies involved, there is insufficient evidence to robustly test the quality of all applicants. To ensure that top quality A level students are attracted, participating companies suggested that more marketing needs to be done in schools and with parents.
The onboarding of students **How successful was this?** **What more could have been done?**	The onboarding process is completed by the QA talent team. For cohort 1 this involved the completion of sign up forms by post or email followed by telephone calls that could take up to 2 weeks to complete (for example to obtain evidence of the required qualifications). This was changed to an online process for cohort 2 where the talent team sent out links for completion of academic achievement and work experience which was passed to the QA compliance team for approval and confirmation of funding eligibility before being sent to the delivery team. Skills Coaches complete the enrolment on the programme. While the majority of apprentices that provided feedback rated their workplace induction as good or very good (n=13, 68%) they highlighted that the onboarding and induction process could be improved to incorporate more detail on the objectives of the apprenticeship, with less focus on the company.
Regular interaction with students through the Skills coaches	Companies and apprentices indicated dissatisfaction with the technical knowledge of the Skills Coaches, noting that on some occasions their feedback on apprenticeship course work, when reviewed by apprentice line manager or technical mentor, was deemed incorrect.

[79] QA (2018) Cyber Security Apprenticeship Recruitment – Phase 2 End of Campaign Review

Research question	Key findings
Did the review meetings take place? **What was students' feedback of the skills coaches and interaction?** **Were there any issues?**	Both employers and apprentices also highlighted there was insufficient communication on the progress of the apprentices against programme requirements. In addition, employers felt that the regular meetings with the Skills Coaches lacked sufficient structure and did not add value.
Quality of learning training provided and locations **Did the training provided meet the objectives of the learning?** **Could more/less be done?**	The majority of participating employers that provided feedback felt that the training met the objectives of the learning and was of good quality, with one employer noting 'apprentices felt they were getting good quality tutors who were able to help them and convey the material at the right level'. Moreover, both companies and apprentices felt that allocating time to training and learning on a weekly basis was more beneficial than assigning training time in larger blocks as it allowed for it to be applied on a more continuous basis. Of the 19 apprentices that provided feedback 95% (n=18) were satisfied or very satisfied with the time they had for training.
The creation and success of the criteria and training **Was this aligned to the standard?**	Companies and apprentices expressed concern that the course content, syllabus and the level 4 apprenticeship standard (assessed via the BCS end point assessment) did not align.
The success of the individual learning plan **How did this go?** **Was this utilised fully?**	There were mixed views from apprentices on the usefulness of the learning plan, with more apprentice respondents from cohort 1 suggesting it was beneficial (75% of cohort 1 respondents believed it was useful or somewhat useful while 80% of cohort 2 apprentice respondents felt it was of little or no use).
Support from employer, including engagement with students, point of contact in organisation **How did employers interact with students?**	All employers who provided feedback noted that they provided a range of support to their apprentices on the programme, including mentoring, pastoral care, additional training related to their business area and funding for certifications. Of the 19 apprentices that provided feedback 17 (90%) were satisfied or very satisfied with the support provided by their employer.
End point assessment **How did this go?** **Did all students achieve what as expected?** **Could more advice have been given?**	At the time of providing feedback, some of the apprentices were still completing their end point assessment. Of those that did provide feedback (n=2) one stated they achieved what they expected however the second noted that the end point assessment did not go as planned due to a lack of understanding of the apprenticeship and synoptic project by the interviewer **(Note – BCS were invited for interview however were unable to take part in the evaluation).**
Overall Project Management **What improvements could be made to risk management, management information, governance and the tracking of progress?**	While general updates on the programme and learner progress were provided by QA to DCMS there was no centralised governance or formal, documented reporting against the measures set for performance. Companies also highlighted they would have liked greater governance / monitoring of the programme by DCMS, in particular to help resolve issues around quality of training delivery. They would have liked greater intervention from DCMS as the funding body in monitoring the performance of the training provider and ensuring quality.

5.4 Outcomes achieved

Apprentices were asked to rate how confident they felt in several areas related to the role of a Cyber Security Technologist and respondents indicated that from a combination of course material and on the job training provided:

- 68% (n =13) felt confident or very confident to take on a range of tasks to identify risks (for example researching, investigating, analysing and evaluating security threats)
- 32% (n =6) felt confident or very confident in undertaking security risk assessments, without direct supervision
- 32% (n =6) felt confident or very confident in mitigating and responding to cyber threats
- 26% (n=5) felt unsure or very unsure about how to mitigate and respond to cyber threats
- 26%(n=5) felt unsure or very unsure about how to develop systems using cryptography / key management

Participating companies stated they were satisfied with the progress made by their apprentice and felt they had helped to:

- increase their cyber security capacity
- improved their ability to identify cyber security risks, protect devices / systems and detect / respond to cyber-attacks
- highlight the need to think more about cyber security issues relative to their business and increase the cyber security knowledge of the wider team. In one instance apprentices were involved in delivering cyber security presentations at learning engagement days across the wider business and were successful in communicating technical information to non-specialist audience. In another company apprentices have been registered as cyber security ambassadors to complete outreach work in schools
- encouraged them to think about future needs in relation to cyber security
- demonstrated that their company is committed to investing in cyber security

5.5 Alignment to the standard

The following table outlines a curriculum mapping of the level 4 cyber security technologist course provided against the apprenticeship standard.

Overall it is evident that while the learning outcomes are all covered, there are some which are covered in a more lightweight or superficial way (e.g. future trends). It is also the case that several of the modules have no relation directly to the standard: module 2, 5 and 6 are in that case. In particular, there is a lot of content on cryptography which is not mentioned directly in the standard.

Table 6: Curriculum mapping of the level 4 cyber security technologist course

Learning outcomes	Units									
	Module 1: Open Source Intelligence	Module 2: CompTIA Network+	Module 3: CompTIA Security+	Module 4: BCS Cyber Security Introduction	Module 5: BCS Network and Digital Communications Theory	Module 6: CS Employment of Cryptography	Module 7: ISO27001 Foundation	Module 8: Building a Security Case	Module 9: EC-Council Ethical Hacking and Cyber Forensics Associate	Module 10: Capture the Flag workshop
Discover (through a mix of research and practical exploration) vulnerabilities in a system	X								X	
Analyse and evaluate security threats and hazards to a system or service or processes			X				X		X	X
Research and investigate some common attack techniques and recommend how to defend against them			X						X	X
Undertake a security risk assessment for a simple system							X			
Source and analyse a security case								X		
Develop a simple security case without supervision								X		
Identify and follow organisational policies and standards for information and cyber security			X				X		X	
Operate according to service level agreements or employer defined performance targets			X				X		X	
Investigate different views of the future (using								X (loosely)		

Learning outcomes	Units									
	Module 1: Open Source Intelligence	Module 2: CompTIA Network+	Module 3: CompTIA Security+	Module 4: BCS Cyber Security Introduction	Module 5: BCS Network and Digital Communications Theory	Module 6: CS Employment of Cryptography	Module 7: ISO27001 Foundation	Module 8: Building a Security Case	Module 9: EC-Council Ethical Hacking and Cyber Forensics Associate	Module 10: Capture the Flag workshop
more than one external source) and trends in a relevant technology area										
Why cyber security matters				X						
Basic theory – concepts such as security, identity, confidentiality, integrity, availability, threat, vulnerability, risk and hazard				X						
Security assurance				X			X			
Deriving security objectives with reasoned justification in a representative business scenario							X	X	X	
Cyber security concepts applied to ICT infrastructure			X							
Attack techniques and sources of threat								X	X	X
Cyber defence								X	X	X
Relevant laws and ethics							X		X	
The existing threat landscape			X	X				X	X	
Threat trends				X				X		X

5.6 Conclusion

There are a number of learnings that can be taken forward into any future support. Area of the programme that worked well include:

- **Learning and training** – participating employers felt that the training met the objectives of the learning and was of good quality
- **Support from employer** – employers provided range of support to their apprentices on the programme and apprentices were satisfied with support provided

Key areas for development include:

- **Marketing** – needs to be significantly improved to ensure the programme is promoted to employers, with detail on the cyber security risks and how these skills and cyber security apprenticeships can help. Case studies of how apprentices help companies should be used to promote the programme
- **Onboarding of students / induction process** – could be improved to incorporate more detail on the apprenticeship
- **Communication, engagement and support provided by the Skills Coaches** - the roles and the support provided by Skill Coaches needs clarified; and the management of Skills Coaches improved
- **Learning and training** – could be expanded to include more analyst content and greater clarity on how the course content maps the level 4 apprenticeship standard (assessed via the BCS examinations end point assessment). The course content should be reviewed given the issues raised on alignment to the standard and to BCS end point assessment
- **Individual learning plan** – needs developed to add more value to the apprentices on the programme

Overall Project Management – needs development to ensure delivery issues are resolved as they arise. There needs to be more formal, documented reporting process to monitor programme delivery.

6. OPTIONS AND THE WAY AHEAD

6.1 Introduction

This section sets out several options that have been considered as potential interventions to develop a sustained supply of home-grown cyber security talent to help meet cyber security skills gaps in the UK and in particular the CNI sector.

6.2 Options reviewed

Based on the evidence collected from the survey and consultation work, 4 options were considered as potential interventions and a brief summary of each is outlined in the following table.

Table 7: Summary of proposed options

Option	Summary
Option 1 (existing scheme - status quo)	Involves a level 4 cyber apprenticeship programme for CNI sector companies.
Option 2 (level 6 cyber security technical professional for the CNI sector)	This option was suggested by employers in CNI and involves DCMS funding a level 6 cyber security technical professional degree apprenticeship (to include aspects of cyber security as well as core digital skills) or level 7 digital and technology solutions degree apprenticeship. The choice can depend on the specific needs of the company.
Option 3 (level 4 cyber security apprenticeship for the non – CNI sector)	Involves DCMS funding a level 4 cyber security apprenticeship for non - CNI sector companies to recruit new cyber security staff. The content would be the same as option 1 and is based on the research that shows high levels of basic technical skills gaps are more evident in the food or hospitality; construction; retail or wholesale; and professional scientific or technical firms.[80]
Option 4 (accredited tailored interventions to transition existing employees into new cyber security roles in the CNI sector)	This option was based on feedback from employers and involves DCMS providing funding for companies to retrain existing employees into new cyber security roles. The level of support required will depend on the skill gaps within individual companies / sectors.

[80] Ipsos Mori (2018) Understanding the UK Cyber Security Skills Labour Market

6.3 Summary options assessment / preferred option

Assessment criteria were developed in order to identify the best approach to addressing the market failures in a cost-effective way and discussed with the project Steering Group. The criteria are outlined below and each option was assessed against each criterion.

Table 8: Assessment Criteria

Assessment criteria	Indicators
Employer need/ buy in	Employer buy in based on feedback collected from employers participating in option 1 (status quo). For other options it can be surmised based on key stakeholder feedback. Note: Insufficient research has been completed on employer need and demand, however this work is being developed further by the Digital Skills Partnerships (DSPs).
Demand from cyber security apprentices / trainees	Evidence of actual or projected demand from apprentices / trainees.
Fit with wider apprenticeship and cyber security policy landscape	Link to apprenticeship and cyber security policy / strategic objectives.
Cost to government	Costs outside the apprenticeship levy.
Additionality	Extent to which companies would have taken on apprentices or trainees without intervention.
Outcomes	Assessment of evidence available as to whether the intervention has or will deliver the cyber security skills/ expertise needed by CNI sector.
Coverage and scope	Ability to be provided at scale (either across all 13 CNI sub sectors or all sectors, depending on the option requirements).
Does not increase complexity in the market / sector	Addition of any new support should not add to the complexity which is starting to emerge in cyber security skills/ education.

The following table provides a summary of the assessment scores for each option. The assessments reinforced that the cyber security industry is at an early stage of development and there is a lack of evidence on the skills required. This information is difficult to collect as many employers are unclear as to what their cyber security requirements are. This information will develop over time as the market matures, however in the interim it is necessary to pilot different approaches in a cost-effective way to learn what works and does not work for different employers.

Table 9: Options Summary - Scored

Assessment criteria	Option 1 (existing scheme - status quo)	Option 2 (level 6 cyber security technical professional for the CNI sector)	Option 3 (level 4 cyber security apprenticeship for the non – CNI sector)	Option 4 (accredited tailored interventions to transition existing employees into new cyber security roles in the CNI sector)
	Score	Score	Score	Score
Employer need/ buy in currently	Low / Medium	Medium/ but untested	Evidence not available	Medium/ but untested
Demand from cyber security trainees/ employees	High	High	High	Evidence not available
Fit with wider apprenticeship any cyber security policy landscape	Medium	Medium	Medium	Medium
Cost to government	High (see notes 1 and 2 below)	See note 2 below[2]	See note 2 below	Lows score/ high costs
Additionality	Low (due to a small amount of evidence)	Evidence not available (see note 3 below)	Evidence not available	Evidence not available
Outcomes	Low	Evidence not available	Evidence not available	Evidence not available (see note 4 below)
Coverage and scope	Low	Low	Low	TBC (see note 5 below)
Does not add to the complexity that exists in the market / sector[81]	High	High	High	Low

Notes:

1. Cost to government is low based on apprentice marketing and recruitment costs only (apprenticeship delivery is supported by the apprenticeship levy) and limited marketing to employers

2. Under this option increased investment is needed to increase knowledge and awareness of cyber security skills and how they help reduce cyber security risks to companies

3. Could potentially displace people to university to study a cyber security underg raduate or post graduate degree

4. However Australia is promoting the use of transition models to transition workers from the broader IT sector and other industries into cyber security roles

5. Coverage / scope would depend on the interventions funded

[81] High score means the risk of increasing complexity in the market is low

Table 9 highlights that the options available are varied, however as employer demand/ buy in is unclear it is difficult to identify a best option. Given the early stage development of cyber security skills and the need to find a solution to address the cyber security skills gap, especially for the CNI sector, it is important that government continues to pilot programmes and build the evidence base as to what works and thereafter implement the learnings.

6.4 Preferred option

There are gaps in the information available and therefore insufficient data to make clear recommendations on which option is preferred.

Employer buy in is critical to delivering a cost-effective apprenticeship intervention in this space. However, as many companies are unclear as to their cyber security skill needs or how the apprenticeship levels fit with any needs they may have, there are a number of areas that need actioned. The piloting of different schemes and interventions allows companies the opportunity to trial new apprenticeship levels. Therefore, further evaluation work will be required to assess if it addresses the identified market failures in an effective way.

Delivery

The options outlined above could be delivered using an employer / industry led or a government led approach.

Government led approach – the cyber CNI apprenticeship programme used a 'government led' approach as DCMS were responsible for the management of the programme and provided a link between employers and the training provider. This approach also meant employers were 'recruited' onto the programme rather than companies seeking the type of apprentice that would meet their company's needs. While the government led approach was appropriate to try to stimulate the market to prioritise cyber apprenticeships, it meant less direct engagement between the employer and training provider than normally occurs in apprenticeship delivery and resulted in confusion on roles and responsibilities. Going forward, an alternative approach may be for government / DCMS to focus on providing support to create a market demand for apprentices rather than focus on the project delivery aspect/financial funding.

Employer led approach – an 'employer / industry' approach involves companies having responsibility for seeking the apprenticeships that fit with their company needs and directly contracting with the training provider.

The advantages and disadvantages of each approach are set out below:

Approach	Advantages	Disadvantages
Government led approach	The approach used in the cyber CNI apprenticeship programme provided a pilot scheme where none previously existed, allowing companies to trial this most may not have chosen the level 4 cyber security technologist pathway.	Many employers (especially large employers) have apprenticeship systems / processes already in place and as a result prefer to liaise directly with training providers to ensure their needs can be met rather than going through another organisation. The training provider is more easily able to focus on employer needs rather than metrics that often need to be included in a public sector contract to demonstrate accountability for public monies.
Employer led approach	Gives the employer greater responsibility and ownership of the training and the opportunity to develop relationships with the training providers. The importance of establishing a productive employer / trainer relationship is highlighted in recent research[82] on future skills challenges which noted that the linear model of 'education to employment to career' is no longer sufficient. Research[83] suggests that educators and employers need to collaborate more closely and develop new and innovative partnerships and flexible learning approaches, stating that "every effort must be made by government to adopt a whole-skills approach and to embed educator –employer partnerships across policy to support this".	It relies on employers being sufficiently motivated and knowledgeable on how the apprenticeship programme can help their business for them to consider this as an option.

6.5 Good practice

Research[84] has indicated there are more apprenticeship applications than places available. Therefore there is a need for local and national government to convince employers of the benefits of taking on an apprentice, incentivise employers (for example through making requirements of them through public procurement practices), to mitigate the perceived risks and to ensure the quality of the training that employers can access.

The following section outlines examples of actions taken to encourage uptake of apprenticeships.

Social clauses

The use of social clauses is one example of how policy can encourage uptake of apprenticeships. For example, capital build projects procured through the public sector now often include the

[82] Universities UK (2018) Solving Future Skills Challenges

[83] Universities UK (2018) Solving Future Skills Challenges

[84] Demos (2015) The Commission on Apprenticeships

requirement for contractors to provide apprenticeships in line with the size of the contract.[85] This is an action that government could consider for all public sector contracts in relation to cyber security.

This approach was referred to in the second report[86] by the Joint Committee on the national security strategy on cyber security skills and the UK's critical national infrastructure which suggests the development of cyber security skills could be incorporated within public procurement requirements. It recommended that government "[extend] its recent announcement that all principal Government suppliers will be expected to implement certain minimum cyber security standards so that they also incorporate the development of cyber security skills. This would involve writing into Government contracts equivalent criteria for training activity and continuing professional development". This could complement the existing Cyber Essential Scheme, by requiring a certain number of cyber security apprentices linked to the size of government contract.

Flexible apprenticeships

Apprenticeships can often last longer than employers require which may be a barrier to greater uptake of apprentices, particularly amongst small businesses. Shared apprenticeship schemes are one approach to address this as they share the risk among a group of employers. Under this model, apprentices are employed by the managing agency and can complete their apprenticeships on several placements with different employers. Examples include:

- Training and Apprenticeships in Construction (TrAC)[87] - an employer led initiative set up to support employers who are unable to provide employment for the full duration of an apprenticeship or only require apprentices for short term projects
- CITB Shared Apprenticeship Scheme[88] - allows companies to take on an apprentice, for as short a duration as three months, with no commitment to the apprentice at the end. It allows employers to support and benefit from apprentices, even if they are unable to offer them a long-term placement

The flexibility offered by apprentice sharing schemes is particularly important in industries where most employers are SMEs and where longer-term pipelines of work can be uncertain. Evidence from similar schemes in Wales suggests this approach can be successful from the perspective of both employers and apprentices. An independent evaluation[89] (although based on small numbers) found that apprentices who were part of the shared apprenticeship schemes had better completion and better employment rates than apprentices generally in Wales.

Good quality training / good relationship and communication with the training provider

To support the development of effective relationships with the employer some training providers have work based employer engagement advisors. In addition to mentoring apprentices, they have a relationship with employers to ensure that teaching is complementary to employer needs and to

[85] Public procurement of contracts worth £10million or more, which last 12 months or longer, should support skills development and the government's commitment to create 3 million new apprenticeships by 2020. Procurement Policy Note 14/15 provides further details

[86] Joint Committee on the national security strategy (July 2018) Cyber Security of the UK's Critical National Infrastructure

[87] https://www.tracweb.co.uk/ (accessed August 2019)

[88] https://www.citb.co.uk/courses-and-qualifications/citb-apprenticeships/take-on-an-apprentice/types-of-apprenticeships/shared-apprenticeship-scheme/ (accessed August 2019)

[89] Roe, P and Costello, M (2014) Evaluation of Shared Apprenticeship Pilots

ensure that 'there is a strong line of communication between college tutors or assessors and the employer, to enable robust monitoring of the apprentice's progress in the college and work environment'.[90]

Supply chain approach

There are also examples of larger businesses supporting SMEs to offer apprenticeships. Large employers such as Microsoft have developed an employer-led 'supply-chain' approach to designing and delivering apprenticeship programmes. These particularly support smaller employers who do not pay the apprenticeship levy and who may not have the commercial weight to influence training providers, however require a similarly rigorous curriculum and method of delivery to larger employers.

Microsoft Case Study[91]:

In 2009 Microsoft facilitated the development of apprenticeship programmes with input from employers in its Partner Network of 24,000 IT and digital businesses. These are independent companies across the UK that provide a range of Microsoft-related products or services, the majority of which are SMEs. The pilot has subsequently developed into a national programme which has approximately 4,500 apprentices starts annually in Digital Technology roles in around 3,000 Microsoft Partners and Customers, with over 71% of these companies having 250 employees or less.

Learning Partners are a specific sub-set of Microsoft Partners that are authorised to provide training for official Microsoft products and services. Microsoft monitor the quality of delivery by ensuring Learning Partners offer the official Microsoft Curriculum through Microsoft Certified Trainers. This is further reinforced by additional qualifying criteria, such as offering apprenticeship Programmes that include official Microsoft content in line with in-demand Microsoft Channel roles and demonstrating consistency and innovation in delivery.

It is suggested that without the role played by the Learning Partners, Microsoft would not have had the reach to engage with individual employers. It is suggested that the local scope of these providers, supported at a national level by Microsoft and utilising its brand to attract both employers and apprentices, has helped the programme to grow.

6.6 What is happening elsewhere

Key developments in addressing the cyber security skills gaps in other countries (United States (US), Israel, Australia, Singapore and the other devolved nations within the UK) were examined at the start of 2019 and a summary of the key findings are included below. All those examined see the development of cyber security skills as a priority area of work and therefore changes are likely to happen quickly.

The following table provides an overview of what is happening elsewhere based on the desk research and consultation with government representatives..

[90] Demos (2015) The Commission on Apprenticeships

[91] Demos (2015) The Commission on Apprenticeships

Table 10: What is happening elsewhere - summary

Approach	Which countries are doing this	What the UK is doing
Apprenticeships	**US** - in the US cyber security has become increasingly important following the 2017 Executive Order[92] on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. The order highlights the need to "support the growth and sustainment of a workforce that is skilled in cybersecurity and related fields as the foundation for achieving objectives in cyberspace". The US Department of Labor provides several grant opportunities to encourage employers in creating apprenticeship opportunities, specifically: • $100 million in grant funding that is available to non-profit trade organizations, industry or employer associations, educational institutions labor unions, and/or labor management organizations • $1.5 million in grant funding to recruit, mentor, train, and retain more women in quality apprenticeship programs and pursue careers in manufacturing, infrastructure, cyber security, and health care, among other industries[93]	DCMS have provided funding for 2 cohorts of the cyber CNI apprenticeships programme (level 4 cyber security technologist). In addition, GCHQ[94] offer 2 apprenticeships: CyberFirst Degree Level Apprenticeship in Cyber Security (with National Cyber Security Centre[95]) and Software Engineering Degree Apprenticeships.
	Australia - in Australia apprenticeships are also a developing area to address the cyber security skills gap. Following the expert review of Australia's vocational education and training system the Australian government is investing $48.3 million to establish a National Skills Commission and National Skills Commissioner.[96] The Commission will undertake research and analysis of future skills needs and will play a role in promoting apprenticeships, including by collaborating with industry to assess and respond to workforce needs. The Australian Government is also investing $41.7 million in pilot Skills Organisations, to trial new approaches to expand the role of industry in the national training system.	

[92] Executive Order 13800

[93] The Women in Apprenticeship and Non-traditional Occupations (WANTO) Grant Program. https://www.dol.gov/featured/apprenticeship/grants (accessed July 2019)

[94] Government Communications Headquarters (GCHQ) is an intelligence, cyber and security agency

[95] NCSC provides advice and support for the public and private sector in how to avoid computer security threats (parent organisation is GCHQ)

[96] https://www.education.gov.au/skills-and-training-budget-overview-2019-20 (accessed July 2019)

Approach	Which countries are doing this	What the UK is doing
	Australia is currently piloting higher-level apprenticeships[97] and AustCyber has commenced discussions about setting up a cyber security apprenticeship stream in this programme. The Australian government also provides support to encourage employers to provide apprenticeships and learners to avail of these. These include the Support for Adult Australian Apprentices (SAAA) incentive aims to encourage up-skilling adult workers through Australian Apprenticeships, with eligible employers to receive a one-off payment of $4,000.[98]	
Online learning	**US** - In the US there is a stronger culture of self-learning than in the UK. The Department of Homeland Security (DHS) has established the National Initiative for Cyber Security Careers and Studies (NICCS).[99] This initiative provides a cyber security training catalogue that allows learners to target courses, mapped to the National Initiative for Cybersecurity Education (NICE) framework[100], by interest and proficiency level (from 0 – no proficiency to 4 – expert). Thereafter training is tracked and individualised by the learner, allowing them to store all training into a profile.	Feedback from some of the key stakeholder interviews suggested there is a need for greater awareness of where individuals can access information on the cyber security training available, and for this to be mapped to a framework such as the National Institute of Standards and Technology (NIST) Cyber Security Framework for critical infrastructure. Websites such as 'Inspired Careers'[101] detail the job roles within cyber security at trainees, practitioner, senior practitioner, principal and lead levels and others such as 'Find apprenticeship training'[102] details providers close to a particular postcode for a particular standard, it does not give national information about providers against standards.
	Australia - in Australia, a computerised skill testing and career matching tool, WithYouWithMe is being used to find and train the most suitable workers for vacant cyber security roles in the market (for two cyber security pathways: cyber security analyst and pen tester roles). It supports candidates transition through an intensive cyber course that aims to get them job-ready in four weeks.	

[97] An integrated program of structured training and paid work, leading to a VET or higher education qualification at the Australian Qualifications Framework level 5 (diploma) or above, which may or may not be undertaken as a contract of training

[98] National Apprentice Employment Network (2019) 2019-20 pre-budget submission

[99] https://niccs.us-cert.gov/ (accessed March 2019)

[100] The National Initiative for Cybersecurity Education (NICE) provides a blueprint to categorise, organise, and describe cyber security work into speciality areas, tasks, and knowledge, skills and abilities (KSAs)

[101] https://www.inspiredcareers.org/browse-careers/cyber-security/ (accessed March 2019)

[102] https://findapprenticeshiptraining.apprenticeships.education.gov.uk (accessed March 2019)

Approach	Which countries are doing this	What the UK is doing
Partnership working	**US** - the registered apprenticeship-college consortium (RACC) model[103] involves a network of colleges and registered apprenticeship programmes working together to provide enhanced educational opportunities to apprentices. Through the consortium, colleges agree to provide credit for a registered apprenticeship completion certificate towards an Associate's or Bachelor's degree as recommended by a recognised third party evaluator. In addition, the US National Initiative of Cyber Security Education (NICE), led by the US Department of Commerce, is a partnership between government, academia and the private sector that seeks to improve the America's cyber security education, training, and professional development.[104]	Research[105] on the role of further and higher education in cyber security skills development indicates in the UK many FE and HE providers seek to collaborate with industry, either with firms that provide ICT services (Cisco, Microsoft, etc. as well as smaller businesses, for example spin-outs from universities that provide cyber security services) and with companies in the wider economy (e.g. the automotive sector). However, the stage at which industry gets involved in the development of cyber security courses, and the nature and extent of such involvement, can vary widely. The research notes that employers work with FE and HE institutions in many ways in the cyber security field. This includes providing work placements, helping to design courses, providing opportunities for extra-curricular activities, and an involvement in delivering courses are all common forms of engagement. A partnership approach is starting to emerge in the UK via the Digital Skills Partnerships (DSPs). Each involve public, private and charity sector organisations[106], however partnership working at a local regional level is at an early stage and they are beginning to gather data on digital skills / supply and demand issues.
	Israel - Israel's strategy is to integrate academia, the high-tech industry, and the military. Israel's mandatory military service for young adults creates a steady flow of individuals with cyber security expertise.	
	Australia - Australia has taken a partnership approach. Businesses and universities in Australia are working together to address the skills gap. For example, Otus Business[107] is working with Macquarie University in Sydney to create a new cyber security training and education hub[108], which brings together industry experts and university academics to grow Australia's cyber security talent pool. The A$10 million 'Optus Macquarie University Cyber Security Hub' is located on campus providing research; short courses aimed at executives; professional courses; undergraduate degree programmes as well as consultancy services to the private sector and government agencies (however does not involve government funding or intervention) Technical and further education institutions (TAFEs) and universities in Australia have expanded their cyber security program offering in recent years in partnership with industry	

[103] https://www.dol.gov/apprenticeship/pdf/RACC_Overview.pdf (accessed March 2019)

[104] https://www.nist.gov/itl/applied-cybersecurity/nice/about (accessed March 2019)

[105] DCMS (2018) Identifying the Role of Further and Higher Education in Cyber Security Skills Development

[106] For example, in Lancashire the DSP includes local digital businesses, 3 universities, colleges, schools, Digital Lancashire and Lancashire County Council

[107] Optus is the second largest telecommunications company in Australia. Opus Business is Optus' enterprise arm

[108] https://www.mq.edu.au/about/about-the-university/offices-and-units/optus-macquarie-university-cyber-security-hub (accessed March 2019)

Approach	Which countries are doing this	What the UK is doing
	under the Cyber Security National Program. It is planned that TAFEs in every Australian state and the Australian Capital Territory (ACT) will offer a streamlined Certificate IV in Cyber Security and Advanced Diploma in Cyber Security. The new qualifications have been developed in close consultation with industry, including National Australia Bank (NAB), Commonwealth Bank of Australia, ANZ Bank, NBN Co, Cisco Australia and New Zealand, REA Group, BAE Systems, Telstra, Deloitte, CITT, the Australian Information Security Association and ISACA.[109]	
Retraining existing workforce	**Singapore** - in Singapore, the Cyber Security Associates and Technologists (CSAT) Programme[110] is a joint initiative by CSA and Info-communications Media Development Authority of Singapore (IMDA). The CSAT Programme trains and up-skills ICT graduates and mid-career professionals for Cyber Security job roles. Trainees can undergo on the job training programmes and participate in local and overseas attachments identified by the CSAT training partners.	In the UK levy funding can be used to transition or upskill existing employees via apprenticeships, however while the number taking up apprenticeships is increasing it is not at the scale required to address the cyber security skills gap. In addition, the DCMS postgraduate bursaries scheme aims to retrain individuals in cyber security by encouraging people transitioning in their career to undertake a GCHQ certified master's course in cyber security.
	Australia - workers from the broader IT sector and other industries with relevant knowledge, skills and abilities are transitioning into cyber security roles. Between 2011 and 2016, more than 70% of workers who became IT Security Specialists (the only cyber security-specific occupation classification currently tracked by the Australian Bureau of Statistics) came from other IT occupations. Most of those who transitioned between 2011 and 2016 were IT and Telecommunications Technicians, followed by IT network and support professionals, and systems analysts / programmers.[111]	
Career pathways	**US** - the National Institute of Standards and Technology (NIST) sponsors CyberSeek, an online tool launched in November of 2016 that classifies US job openings aligned to the National Initiative for Cybersecurity Education (NICE) Workforce Framework. It aims to provide up to date data on supply and demand in the US cyber security job market via interactive visual tools, including heat maps[112] that show worker demand and supply per state. The website also outlines interactive	In the UK an 'Inspired Careers' careers hub was developed in 2015 with the support of the Department of Business, Innovation & Skills (BIS) and Crest. It is an interactive careers hub for those looking to enter the cyber security industry straight from education, those who want to move into cyber security from other industries, or those

[109] https://www.austcyber.com/news-events/tafe-cyber-security-skills-shortage (accessed July 2019)

[110] https://www.csa.gov.sg/programmes/csat (accessed March 2019)

[111] AustCyber (2018) Australia's cyber security sector competitiveness plan

[112] Allows users to understand supply and demand dynamics for cyber security jobs in their state or metro area

Approach	Which countries are doing this	What the UK is doing
	cyber security career pathways[113] which show jobs within cyber security, common transition opportunities between them and detailed information about the salaries, credentials, and skill sets associated with each role.	already working within the industry who want to further their careers. It aims to attract people to the cyber security profession and highlight the different roles open to them. It brings together information on a range of careers available in the industry as well as actual job and internship advertisements, professional and academic courses, articles, whitepapers and social media advice.

Governments from the countries reviewed have highlighted the importance of developing home grown talent in cyber security.

Cyber security apprenticeship programmes are a potential way to help fill the gap, however they are all at an early stage in design and delivery. In the US cyber security apprenticeships are mainly Support Technician roles while Australia is currently piloting higher apprenticeships. In addition, Australia's cyber security sector competitiveness plan includes an action to establish an apprenticeship model for cyber security that will enable more hiring of graduates, with potential funding through the Skilling Australians Fund. Supporting existing employees to transition into cyber security roles is also being tested as an option to increasing the cyber security workforce. The US indicates the importance of clear cyber security career pathways to ensure it is clear how apprentices can progress within the sector.

The key learning is that the cyber security skills sector is relatively immature in the countries reviewed and new approaches are being tried and tested to identify what works best.

6.7 Impact of government policy on apprenticeships

A recent House of Commons briefing paper on apprenticeships and skills policy in England[114] notes that there were over 900,000 funded apprentices in the 2016 to 2017 academic year, and the Government has set a target of 3 million new apprenticeship starts between 2015 and 2020.

On 6 April 2017 the apprenticeship levy came into effect with all UK employers with a pay bill of over £3 million per year paying the levy. Since the introduction of the funding changes in 2017 there has been a large fall in the number of apprenticeship starts. The report notes there may be several reasons for this, including:

- **complexity of the levy** - some commentators have claimed that the levy itself is too complex and has been viewed as a tax on business as companies are struggling to use this funding. The EEF has reported that only 7% of manufacturers have faced "no challenges" with the levy[115]

[113] Allows users to explore common cybersecurity jobs and identify advancement opportunities within cyber security

[114] Powell, Andrew (2019) Apprenticeships and skills policy in England

[115] EEF (2019) A Levy Price to Pay? The Apprenticeship Levy One Year On

- **inflexibility of the levy** - the funds that are collected by the apprenticeship levy can only be used to pay for apprenticeship training and assessment costs. Some commentators, such as the British Chambers of Commerce (BCC), have claimed that the "inflexibility of the system has made it difficult [for organisations] to spend their levy funds as they see best", and that companies should be able to use these funds on any projects that would result in them upskilling their workforce[116]

- **requiring non-levy payers to pay 10% of apprenticeship costs** - since May 2017, those smaller employers who do not pay the levy have had to pay 10% of the apprenticeship training and assessment costs. When coupled with recent increases in the minimum wage, this can mean that the cost of an apprenticeship to a small/medium sized enterprise (SME) can be high. The BCC has reported that, "for SMEs in particular, the new rules have added to the barriers, complexity and cost of recruiting and training staff"[117]

- **the 20% training commitment** - some employers have suggested that the 20% off-the-job training commitment is too large a requirement – employers have reported that they would need to employ an extra person to cover the apprentice's duties while the apprentice is on training. The Association of Employment and Learner Providers have stated that this commitment is "not workable"[118]

However, since the reforms were put in place in 2017, there has been an increase in the number of apprenticeship starts at higher levels (defined as level 4 and above). In 2017/18, 48,400 (13%) apprenticeship starts were at higher level compared to 36,500 (7% of starts) in 2016/17. In addition, 83% of all starts were in four subject areas: Business, Administration and Law; Health, Public Services and Care; Engineering and Manufacturing Technologies and Retail & Commercial Enterprise.

Consultation Findings

When asked what would make them (or their friends) more willing to apply for apprenticeships 11 apprentice respondents highlighted the following (note respondents could provide more than one response):

- more support from training providers
- more information on the benefits
- more support from employers
- case studies / success stories

Participating companies also suggested the following would help encourage other companies to offer cyber security apprenticeships:

- more support for managing apprentices, noting some companies do not have the inhouse knowledge/skill to support them

[116] Powell, Andrew (2019) Apprenticeships and skills policy in England

[117] Powell, Andrew (2019) Apprenticeships and skills policy in England

[118] Financial Times, Calls for changes to levy scheme after apprenticeship starts tumble, 14 June 2018 (https://www.ft.com/content/f8cfcade-6fac-11e8-92d3-6c13e5c92914) (accessed September 2019)

- more engagement with the training providers
- better career and qualification progression for apprentices
- case studies of success stories and how they benefit an organisation
- increased awareness of how apprenticeships work and how the levy works
- better promotion, marketing and communication

In addition, SME consultees highlighted that some smaller companies are not aware of levy funding available or how they can use it.

6.8 Conclusion

The UK cyber security market is embryonic and constantly changing. As a result, there is a need for government to continue to provide apprenticeship support that can be piloted and tested, in order to build greater knowledge and evidence of employers' needs. This work is essential in order to build case studies on what works and use this to market apprenticeships with other employers to encourage uptake. Information on career pathways, jobs and how they link to apprenticeship standards, marketing job/progression opportunities are all needed. Consideration could be given to requiring businesses bidding for government contracts to take on cyber security apprentices in line with the size of the contract (as in the construction sector).

7. CONCLUSIONS AND RECOMMENDATIONS

This section outlines conclusions based on the evidence collected and recommendations to inform other programmes in this area.

Note - caution should be applied to all survey findings due to the small number of responses.

7.1.1 State of the sector and market failures

a) Lack of company awareness of the cyber security skills needed

The cyber security skills requested by companies vary depending on awareness of cyber security risks; awareness of cyber security skills or roles; and willingness to invest in an appropriate resource or support for their need.

There is a lack of detailed evidence on what cyber security skills are needed by companies in the CNI sectors. The information that exists focuses on basic and high-level skills, however this is not directly linked to the apprenticeship standards. There is also evidence that some companies are not clear on how to assess their cyber security skill needs or how best to fill these.

b) Employment of cyber security apprentices

Recent research[119] notes the prevalence of cyber apprenticeships across the private, public and charitable sectors is relatively low. Interviews completed with employers, professional bodies and training providers as part of this research indicate that many companies are unclear of the benefits of apprenticeships in this specific area.

A recent report[120] by the Federation of Small Businesses (FSB) found that SMEs are critical to achieving the government's target of reaching 3 million new apprenticeships by 2020, however some smaller companies often lack the relevant cyber security skills and resources to recruit, train and supervise apprentices.[121] As a result they try to recruit staff with pre-existing technical skills.

Consultation feedback from one professional body and SME consultees (n=2) highlighted that SMEs may not be considering cyber security apprenticeships due to:

- resource / expertise needed - most do not have the support infrastructure they would need to put in place (the DCMS cyber CNI apprenticeship programme required each participating company to have a line manager and mentor for apprentices). In addition, SME consultees highlighted smaller companies may not be able to provide apprentices with sufficient breadth of experience to support the completion of their portfolio or the management time required to help them develop skills for everyday work (for example, time keeping as well as report writing, problem solving and interpersonal skills)
- financial cost - SMEs do not have the funding they would need to invest (e.g. to cover the apprentice and line manager time). One SME consultee also highlighted that the apprentice

[119] Ipsos Mori (2018) Understanding the UK Cyber Security Skills Labour Market

[120] Fit for the Future (2019) Making the Apprenticeship System Work for Small Businesses

[121] The report notes this was a problem for cyber apprenticeships rather than for general IT apprenticeships, where existing staff were more likely to have relevant skills and knowledge to impart.

training time required could have an impact on the wider team if there were only a small number of cyber security staff working on a project

- lack of information / knowledge - SMEs may not know the skills they need, or the interventions available to address these

Given the importance of the CNI sector to the rest of the economy and society it is important that SME employers are helped to overcome these barriers.

Recommendation 1: There remains a need for government intervention to overcome the market failures and ensure cyber security skill objectives are met. The specific market failures are:

Information failure: many employers are not clear on what their cyber security skill needs are and / or how the level 4 apprenticeship fits with these.

Resource / expertise failure: SMEs often do not have the resource or systems in place to support apprenticeships.

Recommendation 2: We recommend that companies within the CNI sector are provided with information on the cyber security risks, the costs of not being ready to mitigate these and how having the right skills and capacity is essential to improve cyber resilience. Ideally case studies could be used to promote how cyber security skills and expertise benefit companies in the CNI sector.

Recommendation 3: We recommend that greater clarity is needed on the jobs and the skills needed by CNI companies and how they map to apprenticeship levels 3 to 7 (and beyond).

Recommendation 4: We recommend that specific supports are put in place to help SMEs access and support apprentices. Examples of good practice include the construction sector where almost three quarters of construction sector SMEs (73%) currently employ apprentices, which is higher than the proportion of SMEs employing apprentices across all sectors (65%).[122] Current initiatives include the CITB Shared Apprenticeship Scheme[123] which allows companies to take on an apprentice, for as short a duration as three months, with no commitment to the apprentice at the end. It allows employers to support and benefit from apprentices, even if they are unable to offer them a long-term placement.

Recommendation 5: We recommend that DCMS work with the Institute of Apprenticeships to ensure that SMEs, in the CNI sector particularly, are made aware of any new developments to support them engage with cyber security apprenticeships.

7.1.2 Success of the programme

Success of the programme is based on reviewing uptake levels, quality of delivery, project management and the outcomes achieved.

[122] https://www.showhouse.co.uk/news/nearly-three-quarters-of-construction-smes-employ-apprentices/ (accessed September 2019)

[123] https://www.citb.co.uk/courses-and-qualifications/citb-apprenticeships/take-on-an-apprentice/types-of-apprenticeships/shared-apprenticeship-scheme/ (accessed September 2019)

Uptake

Companies - the marketing of the programme to employers was limited to a ministerial letter[124] to companies in the CNI sectors alongside DCMS using their existing contacts with CNI employers and via working groups. This was initially focused on energy, transport and defence organisations and was expanded to include more sectors[125] for cohort 2. Feedback from participating companies suggests direct engagement was helpful in getting them involved, however this element of the programme was significantly under-resourced. The marketing of the programme needs to be more extensive, ensuring that more companies are informed of the programme, while also being given information on cyber security risks and the ways in which cyber security apprentices can address these. The introduction of levy funding in April 2017 also impacted on company involvement as DCMS stakeholder feedback noted companies often did not understand how it would work. As a result, companies were less keen to take on and invest in an apprentice at this stage in the levy implementation.

The timing of apprentice recruitment had a detrimental impact on both company and apprentice involvement. In cohort 1 the timing of the National Cyber Security Programme (NCSP) business case cycle meant a confirmed offer of support could not be given to employers before April 2017. Ideally offers would have gone out in early autumn 2016, when firms were completing their financial planning for the year ahead. In addition, it often takes time to equip companies with the knowledge to make decisions on new apprentices and they require a longer lead in time from initial contact by DCMS. For apprentices in cohort 1, feedback from the training organisation (QA) indicates the timing of the application process was also a key issue as the requirement for cohort 1 learners to be signed up by 24 April 2017 created a 'rushed process'.

Apprentices - there were a significant number of eligible apprentice applicants for both cohorts (1,024 in cohort 1 and 1,164 in cohort 2), resulting in 51 apprenticeships in total. Therefore, the current promotional activities for apprentices appear effective. However, the application process involved six stages[126] which may be disproportionate for the level of apprenticeship involved and may not work for both larger and smaller organisations as their recruitment processes will differ. The overall conversion rate (i.e. from completing the application form to offers being made) was 3% as due to the lower than anticipated number of employers, there were a limited number of apprenticeship places available. As a result, the original target of 150 new apprentice starts was not met. Data on the total number of candidates meeting the requirements to reach the final stage of the process was not available from the recruitment organisation within the timeframes of this project. Of the 51 apprentices who joined the programme 7 dropped out, resulting in an expected completion rate of 86%[127]. As apprentices are still completing their end point assessments, it is not yet possible to report a final pass rate for the programme.

Recommendation 6: We recommend that marketing materials setting out the benefits to employers of using cyber security level 4 apprentices are developed and made available to employers across the CNI sector.

[124] 40 companies were initially contacted in autumn 2016 and an additional 100 were written to via a ministerial letter in 2017

[125] Expanded to include water, telecoms, cyber and media

[126] The selection process for the programme included: eligibility questions; application form; Capp's online assessment suite telephone interview; video interview; final assessment stage or assessment centre

[127] Based on 7 apprentices dropping out, it is estimated that 44 will complete the programme (44 / 51 = 86%)

Recommendation 7: We recommend DCMS consider involving the Digital Skills Partnerships in marketing programmes to local employers in their areas.

Delivery of training and support

Most participating employers that provided feedback felt that the training provided by QA[128] met the objectives of the learning and was of good quality, with one employer noting "apprentices felt they were getting good quality tutors who were able to help them and convey the material at the right level".

Moreover, both companies and apprentices felt that allocating time to training and learning on a weekly basis was more beneficial than assigning training time in larger blocks as it allowed for the learning to be applied on a more continuous basis. Of the 19 apprentices that provided feedback 95% (n=18) were satisfied or very satisfied with the time they had for training.

However, companies and apprentices highlighted a need for greater clarity on how the course content maps to the level 4 apprenticeship standard assessed by the British Computer Society (BCS) end point assessment. In addition, both employers and apprentices highlighted there was insufficient communication on progress of the apprentices against programme requirements, and employers felt that the regular meetings with the Skills Coaches[129] lacked sufficient structure and did not add value.

Recommendation 8: We recommend any future intervention should consider the learnings from this programme, including:

- content alignment – there is a need for greater clarity on how the course content, the BCS end point assessment and the level 4 cyber security technologist standard fit together
- support provided by Skills Coaches – in any future intervention the Skills Coaches should:
  - provide timely guidance and feedback in response to work or queries submitted
  - have clear roles and responsibilities (ideally measurable), the details of which is shared with employers
  - have a standardised approach to ensure face to face meetings between Skills Coaches, employers and apprentices provide sufficient and ongoing feedback (from both the employer and the Skills Coach) on how the apprentices are progressing against the expected standards as well as any gaps or issues outstanding and how to address these
  - receive feedback from employers on performance against their roles, responsibilities and performance measures

[128] There are also several other training providers delivering the level 4 cyber security technologist standard

[129] QA Skills Coaches supported apprentices throughout the programme. They were responsible for: helping apprentices to build their portfolio as the programme progressed; meeting apprentices and their line managers regularly in the workplace to check their progress and provide support where needed; and providing pastoral care

Project management

While general updates on the programme and learner progress were provided by QA to DCMS there was no centralised governance or formal, documented reporting against the measures set for performance. Companies also highlighted they would have liked greater governance and monitoring of the programme by DCMS as the funding body to manage the performance of the training provider and ensure quality.

Recommendation 9: We recommend any future intervention should include the requirement for the training provider to submit regular progress reports to the funding organisation detailing performance against the agreed metrics as set out in the contract.

Recommendation 10: We recommend any future intervention clarify the role and responsibilities of the sponsor, recruitment organisation and training provider to ensure those participating in the programme know what can be expected from each.

Outcomes achieved

Apprentices were asked to rate how confident they felt in several areas related to the role of a Cyber Security Technologist and respondents indicated that from a combination of course material and on the job training provided:

68% (n =13) felt confident or very confident to take on a range of tasks to identify risks (for example researching, investigating, analysing and evaluating security threats)

32% (n =6) felt confident or very confident in undertaking security risk assessments, without direct supervision

32% (n =6) felt confident or very confident in mitigating and responding to cyber threats

26% (n=5) felt unsure or very unsure about how to mitigate and respond to cyber threats

26% (n=5) felt unsure or very unsure about how to develop systems using cryptography key management

7.1.3 Other interventions and the way ahead

Four options were considered as potential interventions to provide a sustained supply of home-grown cyber security talent to help meet cyber security skills gaps in the UK and in particular the CNI sector:

- Option 1 (existing scheme - status quo) - involves a level 4 cyber apprenticeship programme for CNI sector companies
- Option 2 (level 6 cyber security technical professional or for the CNI sector) - this option was suggested by employers in the CNI sector and involves DCMS funding a level 6 cyber security technical professional degree apprenticeship
- Option 3 (level 4 cyber security apprenticeship for the non – CNI sector) - involves DCMS funding a level 4 cyber security apprenticeship for non - CNI sector companies to recruit new cyber security staff. The content would be the same as option 1 and is based on research that shows high levels of basic technical skills gaps are more evident in the food or hospitality; construction; retail or wholesale; and professional scientific or technical firms[130]
- Option 4 (accredited tailored interventions to transition existing employees into new cyber security roles in the CNI sector) - this option was based on feedback from employers and involves DCMS providing funding for companies to retrain existing employees into new cyber security roles. The level of support required will depend on the skill gaps within individual companies / sectors

Preferred option

There are gaps in the information available and therefore insufficient data to make clear recommendations on which option would provide the best value for money.

Employer buy in is critical to delivering a cost-effective apprenticeship intervention in this space. However, as many companies are unclear as to their cyber security skill needs or how the apprenticeship levels fit with any needs they may have, employer demand is unclear. The piloting of different schemes and interventions allows companies the opportunity to trial new apprenticeship levels. Therefore, further evaluation work will be required to assess if they address the identified market failures in an effective way.

The UK cyber security market is embryonic and constantly changing. As a result, there is a need for apprenticeship supports to be piloted and tested, in order to build greater knowledge and evidence of employers' needs. This work is essential in order to build case studies on what works and use this to market apprenticeships with other employers to encourage uptake. Information on career pathways, jobs and how they link to apprenticeship standards and job / progression opportunities are all needed.

[130] Ipsos Mori (2018) Understanding the UK Cyber Security Skills Labour Market

Delivery

The options outlined above could be delivered using an employer / industry led or a government led approach.

Government led approach – the cyber CNI apprenticeship programme used a 'government led' approach as DCMS were responsible for the management of the programme and provided a link between employers and the training provider. This approach also meant employers were 'recruited' onto the programme rather than companies seeking the type of apprentice that would meet their company's needs. While the government led approach was appropriate to try to stimulate the market to prioritise cyber apprenticeships, it meant less direct engagement between the employer and training provider than normally occurs in apprenticeship delivery and resulted in confusion on roles and responsibilities. Going forward, an alternative approach may be for government to focus on providing support to create a market demand for apprentices, rather than on the project delivery aspect or financial funding.

Employer led approach – an 'employer / industry' approach involves companies having responsibility for seeking the apprenticeships that fit with their company needs and directly contracting with the training provider.

The advantages and disadvantages of each approach are set out below:

Approach	Advantages	Disadvantages
Government led approach	The approach used in the cyber CNI apprenticeship programme provided a pilot scheme where none previously existed, allowing companies to trial this when they may not otherwise have chosen the level 4 cyber security technologist standard.	Many employers (especially large employers) have apprenticeship systems / processes already in place and as a result prefer to liaise directly with training providers to ensure their needs can be met, rather than going through another organisation. The training provider is more easily able to focus on employer needs rather than metrics that often need to be included in a public sector contract to demonstrate accountability for public monies.
Employer led approach	Gives the employer greater responsibility and ownership of the training and the opportunity to develop relationships with the training providers. The importance of establishing a productive employer / trainer relationship is highlighted in recent research[131] on future skills challenges which noted that the linear model of 'education to employment to career' is no longer sufficient. Research[132] suggests that educators and employers need to collaborate more closely and develop new and innovative partnerships and flexible learning approaches, stating that "every effort must be made by government to adopt a whole-skills approach and to embed educator –employer partnerships across policy to support this".	It relies on employers being sufficiently motivated and knowledgeable on how the apprenticeship programme can help their business for them to consider this as an option.

[131] Universities UK (2018) Solving Future Skills Challenges

[132] Universities UK (2018) Solving Future Skills Challenges

Employers that participated in the cyber CNI apprenticeship programme and provided feedback suggested they were willing to try different approaches to recruiting cyber security staff (i.e. graduates, other apprenticeships or training internal employees). The options above demonstrate that an employer led approach to increasing cyber security skills / resources is likely to be most effective on a large scale, with the role of government as an enabler to support market demand. This could include stakeholder engagement and campaigns to raise awareness of the benefits of taking on and training an apprentice in cyber security.

Recommendation 13: We recommend the continuation of the test and learn approach being used by employers to cyber security apprenticeships in the CNI sector and the collation of evidence of what works and any learnings until the market develops.

Recommendation 14: We recommend that the UK should consider what current programmes (including the apprenticeship levy) could be promoted to employers or could be developed to transition existing employees into cyber security roles. In addition, as part of the cyber security skills strategy DCMS could consider detailing the steps employers can undertake to ensure effective workplace transitions.

rsmuk.com