HM Government

Cyber Security skills: Business perspectives and Government’s next steps

Supporting Evidence

Contents

Purpose of this Document

This document is a companion to the *Cyber Security skills: Business perspectives and Government's next steps* report and supports it by providing the outputs from the questionnaire and feedback from the workshop sessions. This will give interested parties more detailed information on questions asked and where possible provide analysis of the responses received. It also sets out the Government's view on the suggestions put forward by businesses for future actions to strengthen the UK's cyber security skills.

Methodology

The exercise consisted of a series of workshops and an online questionnaire. It was intended to be an extended conversation with a wide range of interested businesses, rather than a research project or quantitative analysis of cyber security skills gaps. Its purpose was to provide an opportunity for structured conversations with both businesses in the cyber supplier sector and businesses that employ cyber security professionals in view of the difficulties they face in recruiting sufficient skilled people. Whilst the primary focus of the exercise was on specialist cyber security skills, discussions also extended to the importance of cyber skills amongst associated professions and the wider workforce, and in particular, board-level decision makers.

Overview of the questionnaire

The purpose of the questionnaire was primarily to ensure that we could capture the views of as wide a range of organisations as possible, including those who did not attend a workshop. It was not expected to (and did not) generate a sample size sufficient to deliver statistically significant results.

An online questionnaire was available 24 hours a day for a month from the middle of November 2013. The questionnaire was accessible using a link to a dedicated survey page on Survey Monkey. The link to the questionnaire was made available and promoted through a wide range of partners and stakeholders including other Government departments, skills organisations and trade associations. Some of the key stakeholders who helped promote the questionnaire are Tech UK, e-skills UK, the IET, Information Assurance Advisory Council, the CPNI (Centre for Protection of National Infrastructure) Information Exchanges, the Retail Cyber Security Forum and Universities UK. Contacts were encouraged to promote the questionnaire through their networks as widely as possible.

Most of the questions in the questionnaire invited respondents to select responses from a drop down list. However, respondents were also given the opportunity to provide free text responses on what more needs to be done to boost the capability of the cyber workforce today and the pipeline of future cyber talent.

Workshops

Four workshops were run in December 2013, with 51 participants representing:

- 17 large cyber suppliers (including some IT and defence companies);
- 12 SME cyber suppliers;
- 17 Critical National Infrastructure companies (energy, finance, transport, telecoms); and
- 5 retail companies and universities.

Participants were invited by BIS, in collaboration with other Government Departments, Tech UK and Universities UK on the basis of their known interest in cyber security. Invitations were also issued to representatives from a number of other business sectors who were unable to attend. The workshops were hosted by BIS, with support from the Cabinet Office, GCHQ, e-skills UK, the Institution of Engineering and Technology (IET) and the Malvern Cyber Security Cluster (SME workshop). The workshops with large cyber suppliers and CNI companies incorporated group discussions and plenary feedback whilst the smaller sessions with SME cyber suppliers and retail/universities were run as round-table discussions. A separate meeting was held with a representative from one SME who was unable to participate in the workshop. Comments were received by email from a representative from one CNI company who was unable to participate in the workshop.

Chapter 1: Questionnaire Outputs

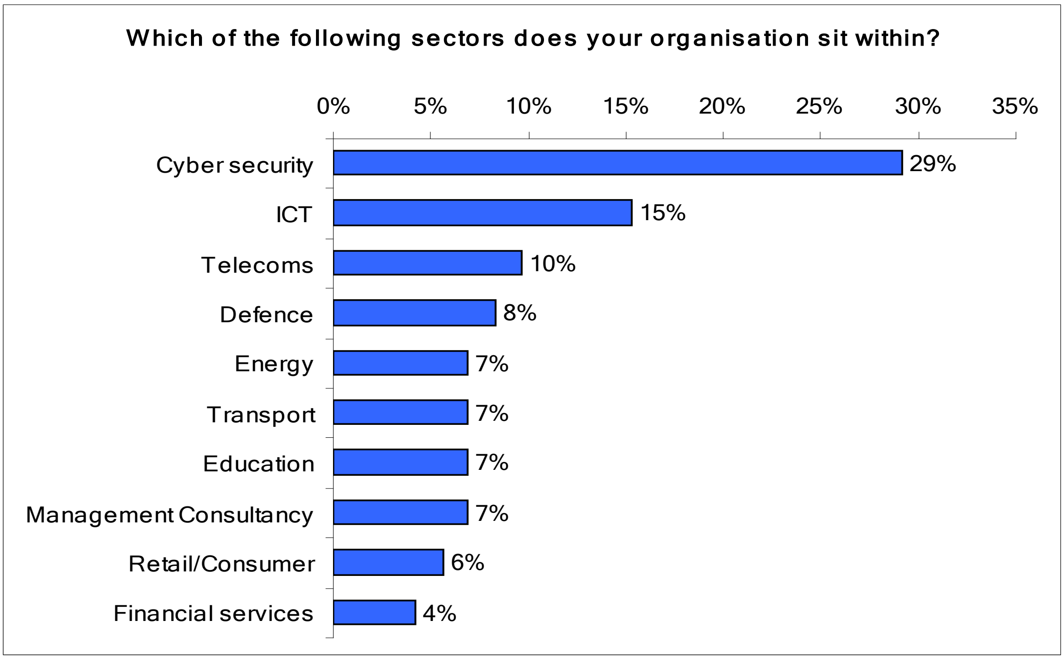
Chapter 1 summarises responses to the questionnaire.

Questions 1 and 4 related to company names and email addresses so responses are not included in this report.

Question 2: Which of the following sectors does your organisation sit within?

Around 30% of respondents who specified a sector were cyber security suppliers. This was closely followed by the ICT sector at 15%. The remainder of respondents fell into a range of sectors, specifically CNI sectors (telecoms, IT, energy, transport, financial services), retail/consumer, management consultancy and education (see chart 1). Additionally, 20% of respondents responding to the question classified themselves as 'other'.

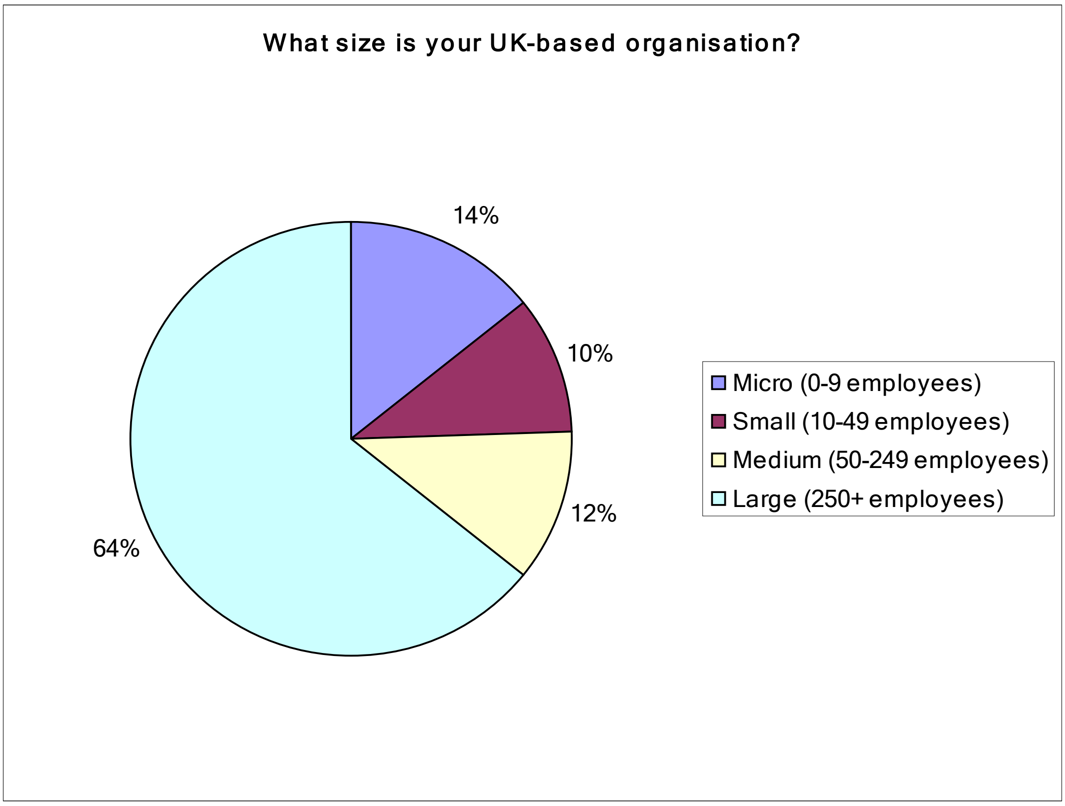
Chart 1:



Question 3: What size is your UK-based organisation?

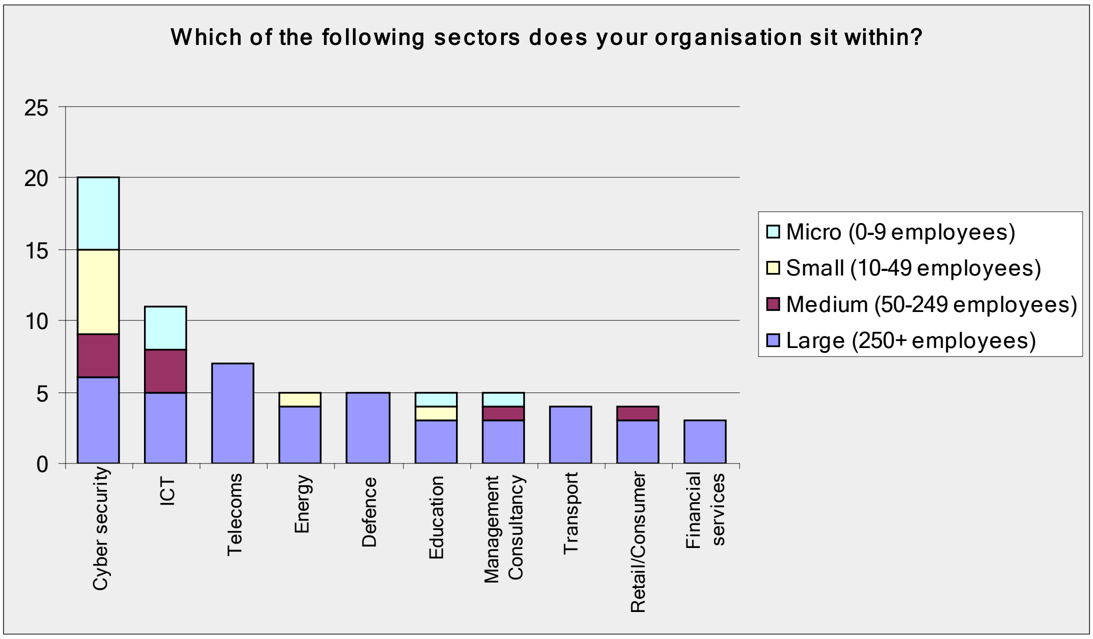
64% of respondents represented large companies (with more than 250 employees), 12% represented medium companies, 10% represented small companies and 14% represented micro companies (see chart 2).

Chart 2:



Most respondents, especially for SME and micro companies, were in the Cyber Security and ICT sectors (see chart 3)

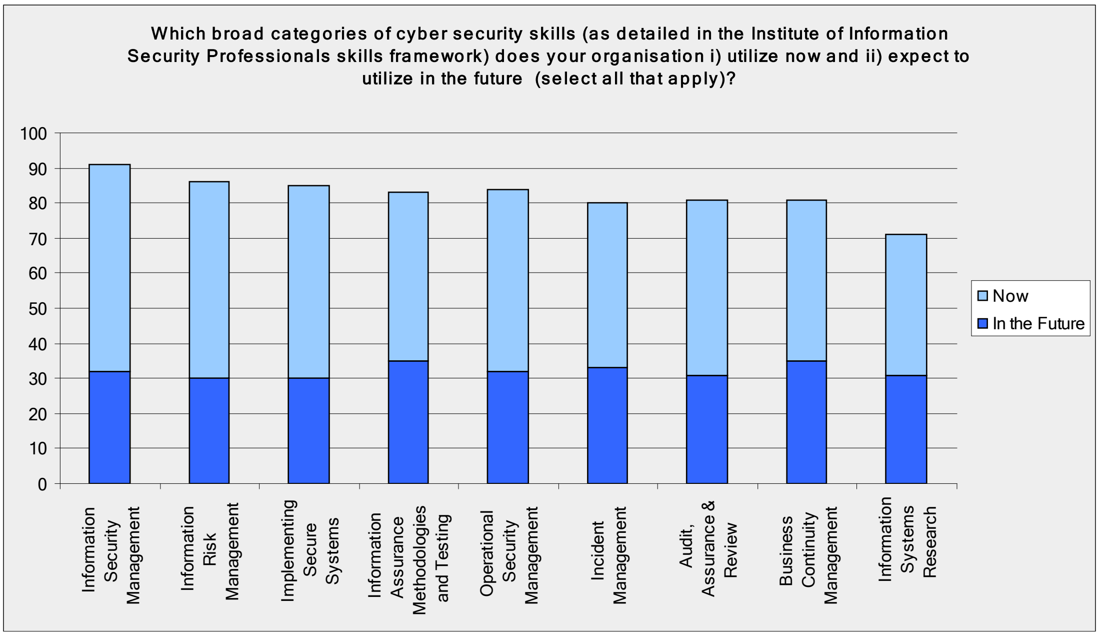
Chart 3:



Question 5 - Which broad categories of cyber security skills (as detailed in the IISP skills framework) does your organisation i) utilize now and ii) expect to utilize in the future (select all that apply)?

Based on the IISP skills framework categorisation, the skills most likely to be used now and expected to be used in the future were information security management (e.g. security management, data protection and compliance), and information risk management (e.g. risk management, threat intelligence) (see chart 4).

Chart 4



Question 6: Approximately what percentage of your organisation's employees do you consider to be cyber professionals (i.e. they have one or more of the IISP cyber security skills)?

Cyber professionals made up less than 1% of employees in around a third of organisations surveyed. They made up between 2 and 20% of employees in around a further third. In around 10% of organisations cyber security professionals made up 81-100% of employees. A higher proportion of employees were cyber security professionals in small and micro organisations than in medium or large organisations.

Chart 5:

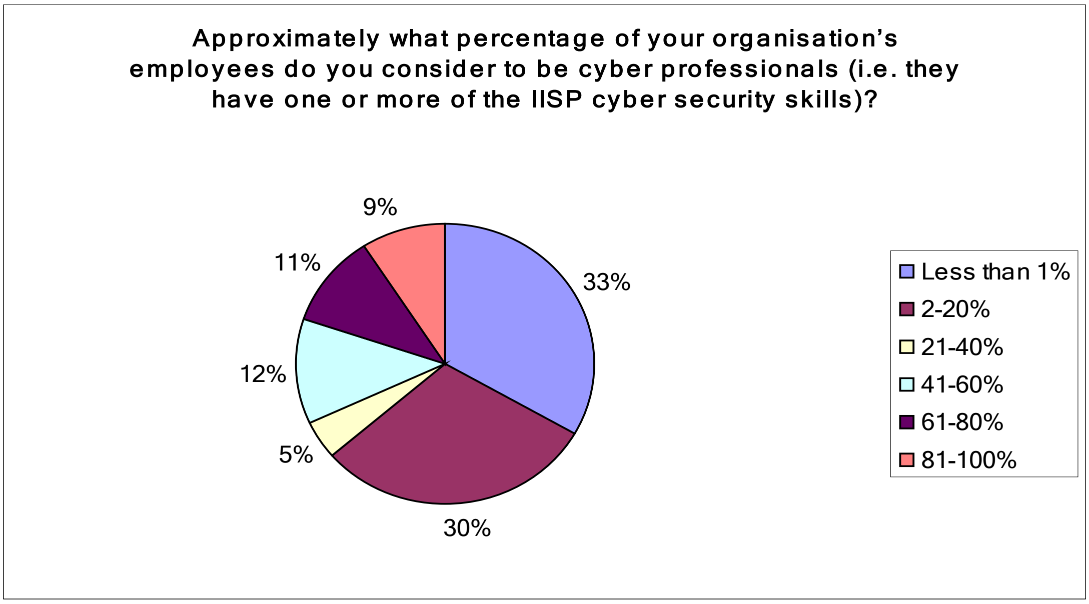
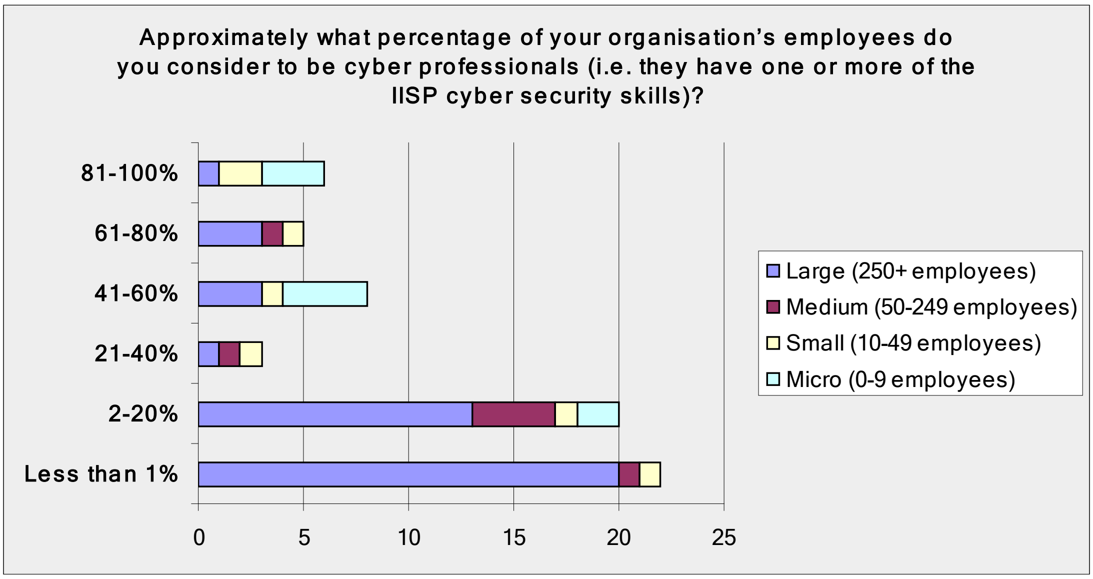


Chart 6:



Question 7 - Which, if any, cyber security skills do you i) find it difficult to recruit for within the UK now and ii) anticipate finding it difficult to recruit for within the UK in the future?

Recruiting for Implementing Secure Systems was seen as the most difficult to recruit for, whist Audit, Assurance & Review and Business Continuity Management (often less technical areas) were seen as the least difficult (see chart 7a and 7b).

Chart 7a:

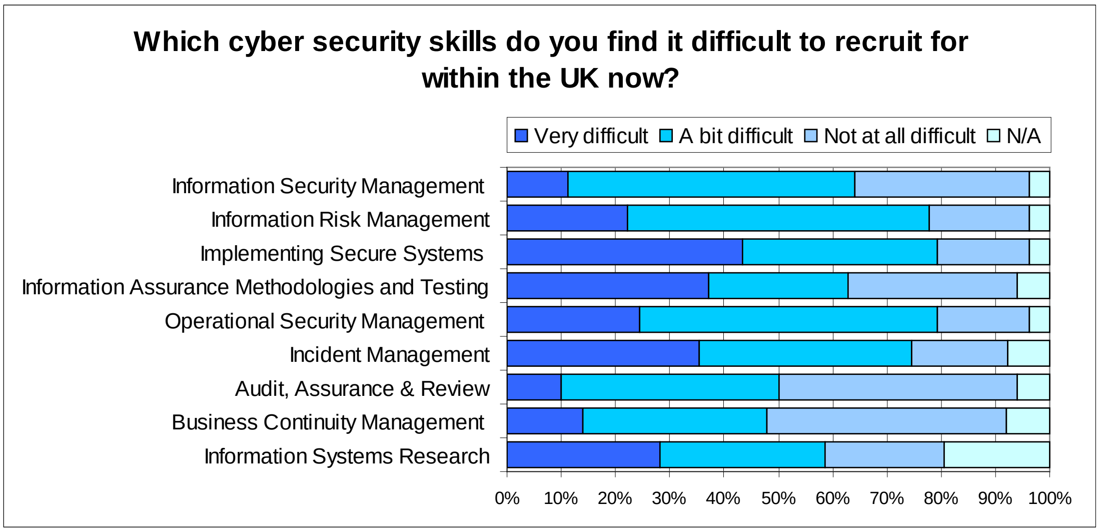
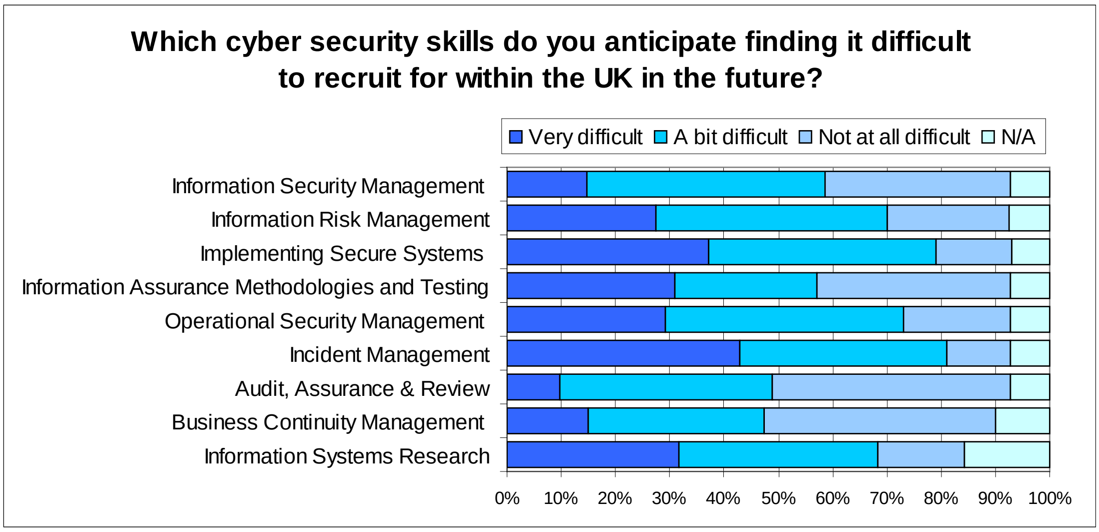


Chart 7b



Question 8: Where do you source cyber security expertise from?

The majority of companies get their cyber security expertise from internal development or recruitment within the UK (see chart 8). In particular Micro companies usually develop or recruit internally with occasional Contractors and Consultants. Small and Medium companies usually recruit externally from within the UK (see chart 9)

Chart 8:

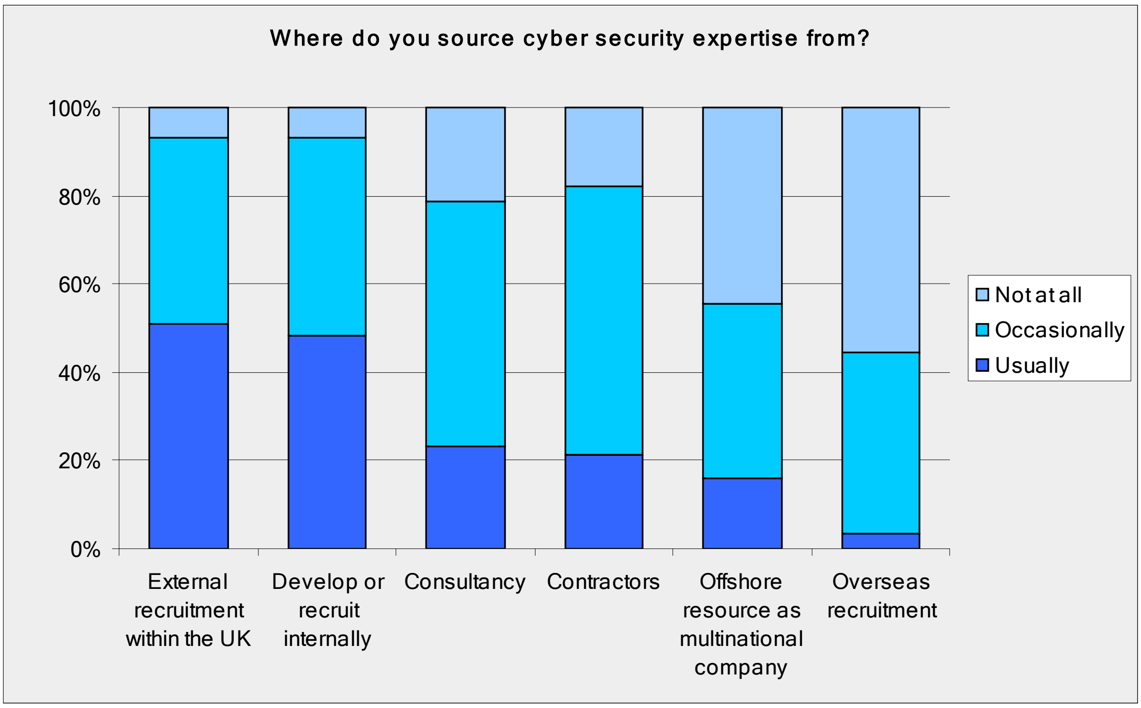
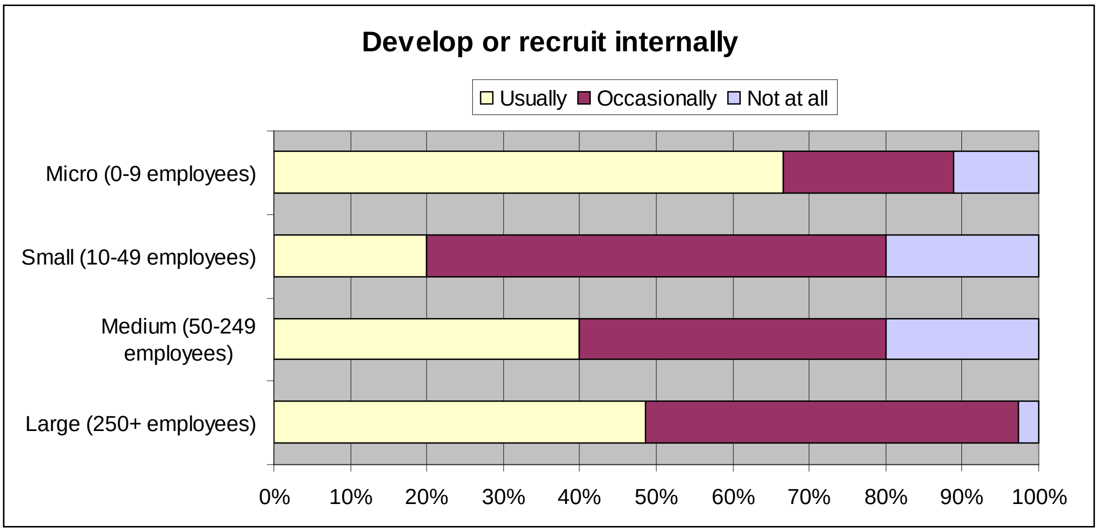


Chart 9:



Question 9 - What types of people do you recruit to fill cyber roles?

Companies usually look to recruit experienced cyber security professionals and only rarely recruit school leavers/apprentices (see chart 10). There were strong similarities on their propensity to recruit new graduates from undergraduate or masters' degrees which echoes commonly held views that companies tend to treat both types of graduates similarly. With the strong value placed on experience, respondents indicated that they were less likely to recruit school leavers or apprenticeships. CNI companies are more likely to recruit temporary contractors/consultants, whist cyber suppliers (including defence suppliers) are more likely to recruit new graduates with undergraduate degrees (see chart 11).

Chart 10:

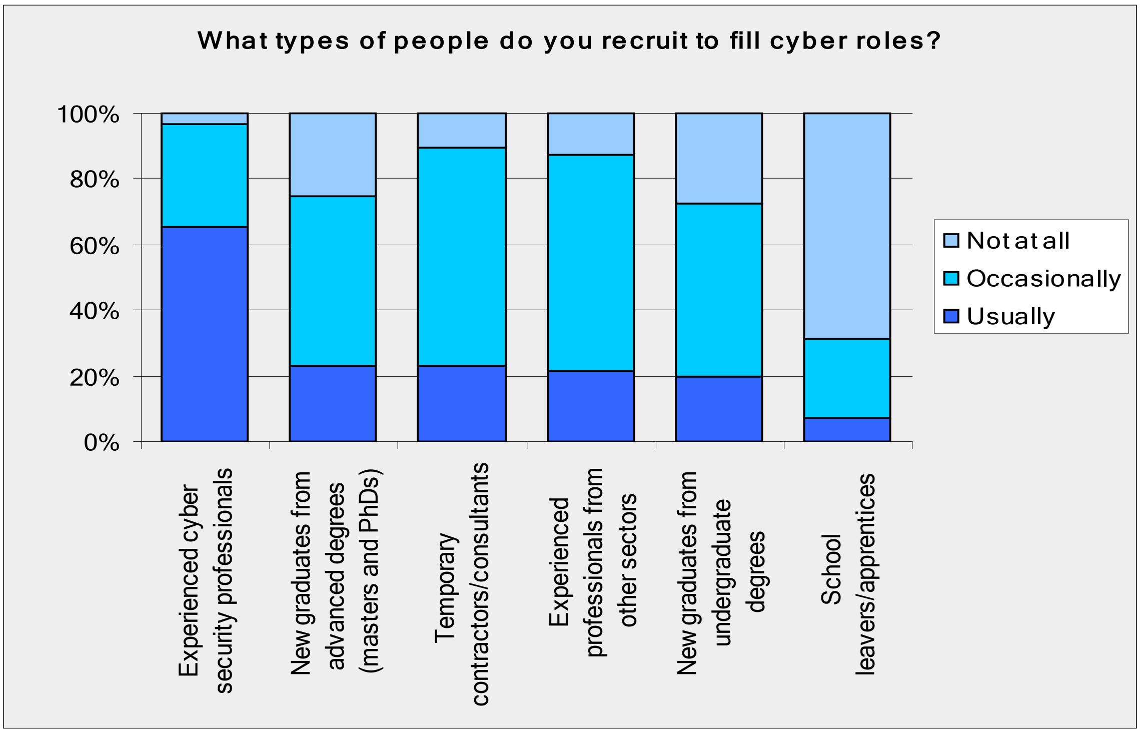
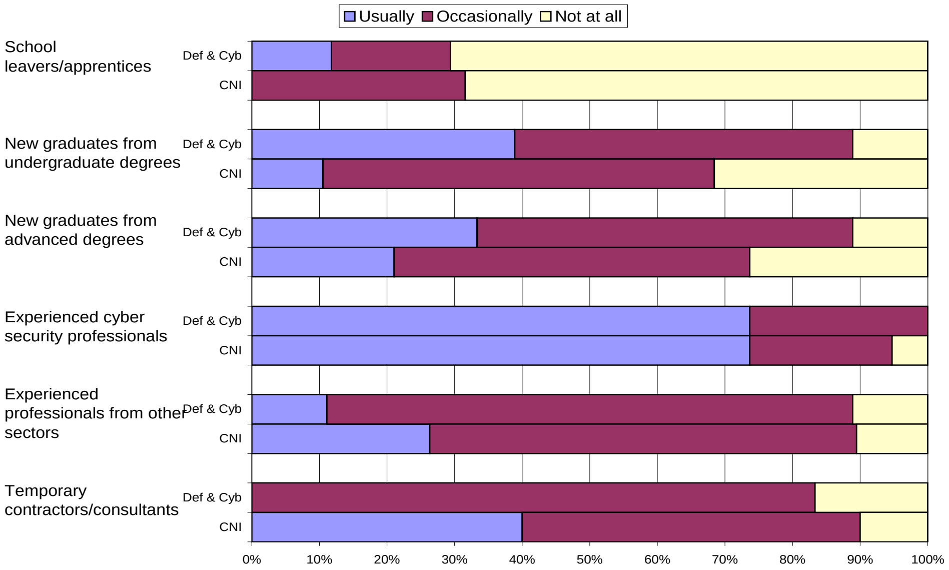


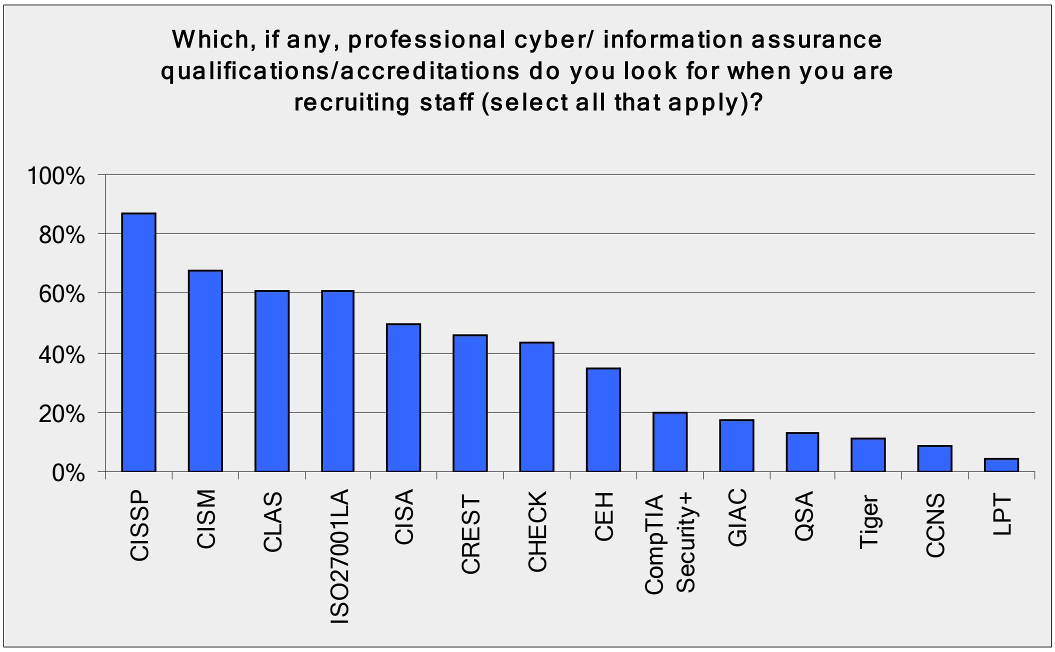
Chart 11:



Question 10: Which, if any, professional cyber/ information assurance qualifications/accreditations do you look for when you are recruiting staff (select all that apply)?

87 per cent of respondents indicated that they would look for as CISSP. This was followed by CISM at 67 per cent and with CLAS and ISO27001LA at 61 per cent (see chart 12). A few respondents selected the ‘other’ category and indicated that they would look for ISSP accreditation.

Chart 12:



CISM is looked for less in Micro, Small and Medium companies compared to large companies (see chart 13) and CNI companies are more likely to look for CIISP and CISM qualifications (see chart 14)

Chart 13:

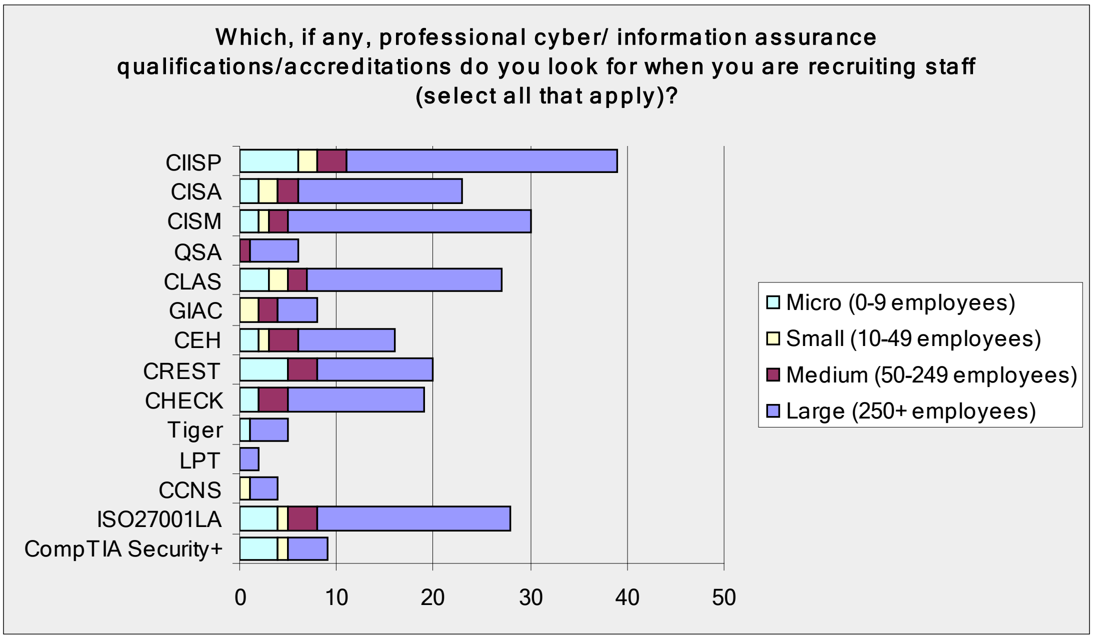
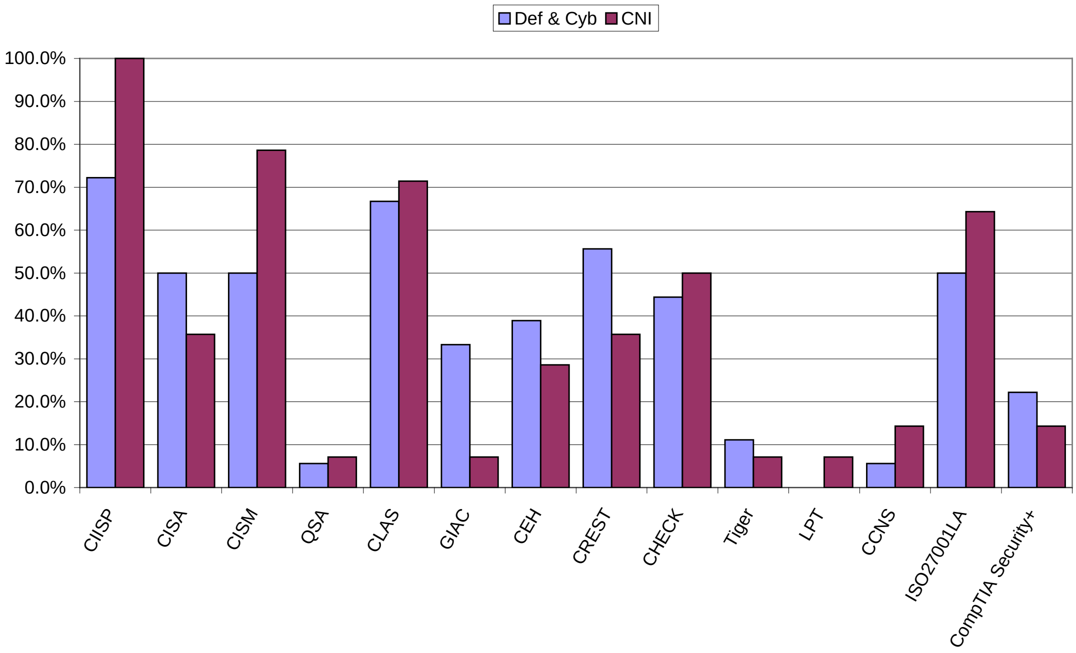


Chart 14



Question 11: Does your organisation oversee or operate Industrial or Process Control Systems (sometimes referred to as SCADA systems)?

About a quarter of large companies oversee and operate Industrial or Process Control Systems. Micro, Small and Medium companies very rarely oversee or operate these (see chart 15). Those who were involved were more likely to carry out in house training of their staff rather than train externally (see chart 16).

Chart 15:

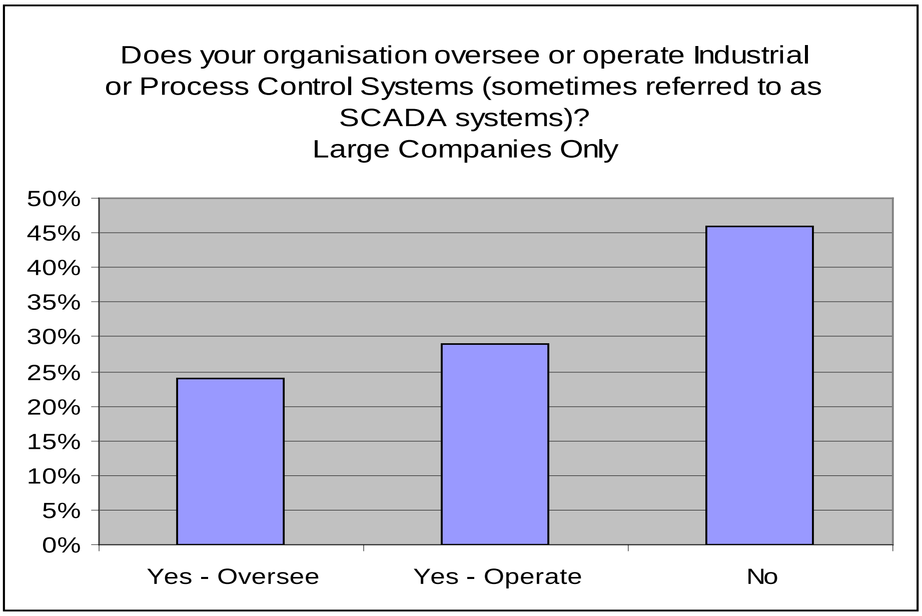
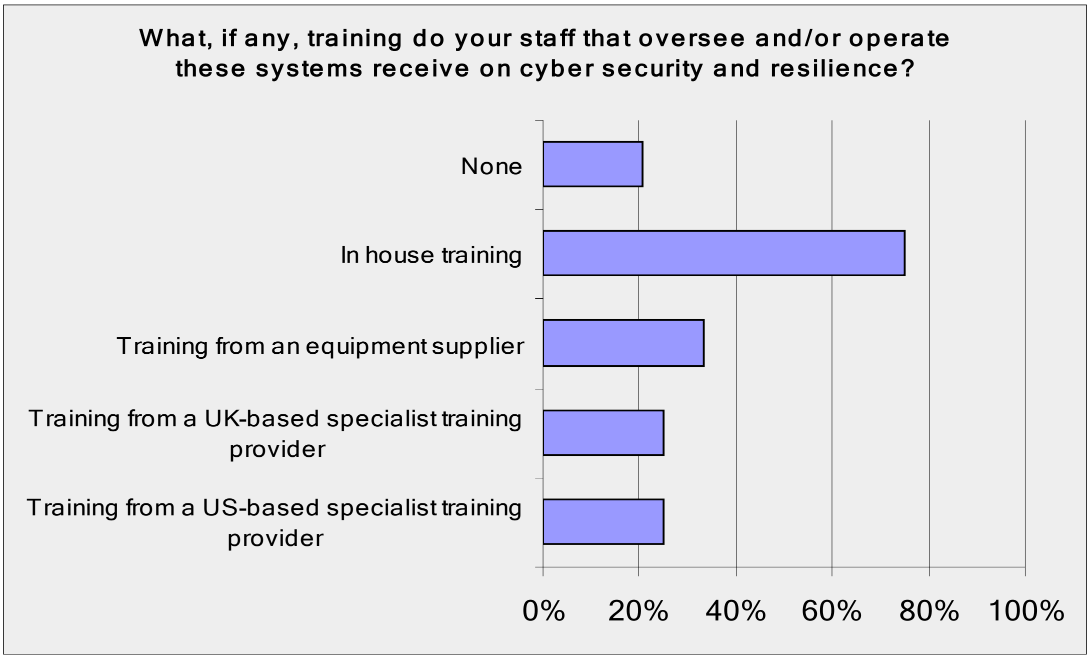


Chart 16:



Question 13: Which of the following activities i) do you currently undertake and ii) would you consider undertaking to support the development of cyber professionals within your organisation ?

Cyber training programmes (both internal and external) were the main ways to support development of current cyber professionals within organisations. The popular ways for supporting future professionals mainly involved business working closely with academia (i.e. advising on cyber skills initiatives), employing students on year long placements, outreach activities with schools and universities and working with universities to help develop or deliver courses (see chart 17).

Chart 17:

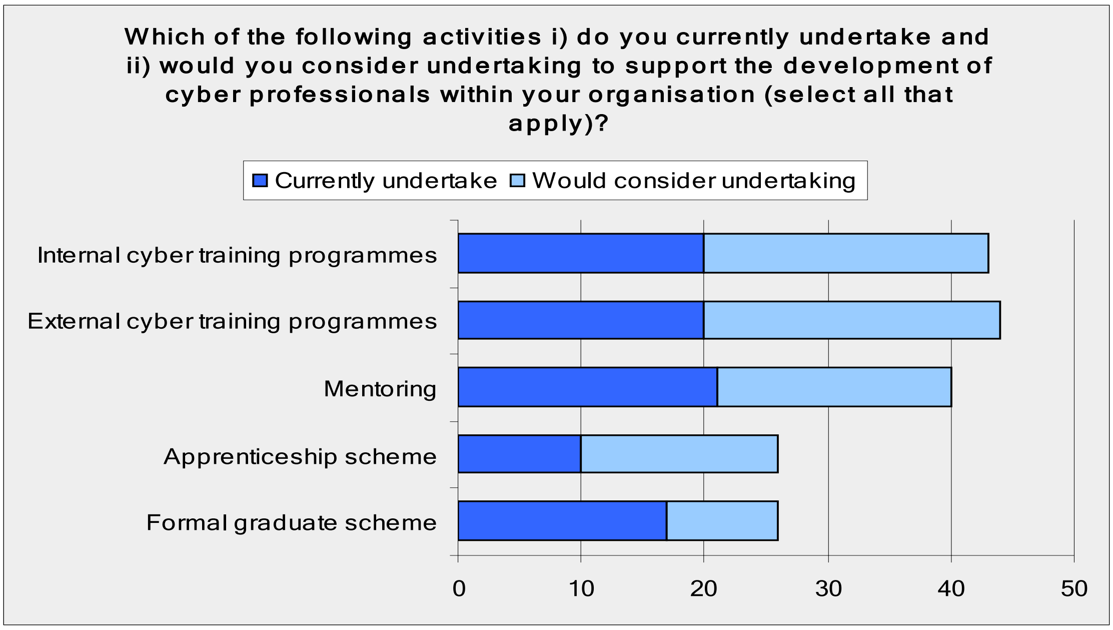
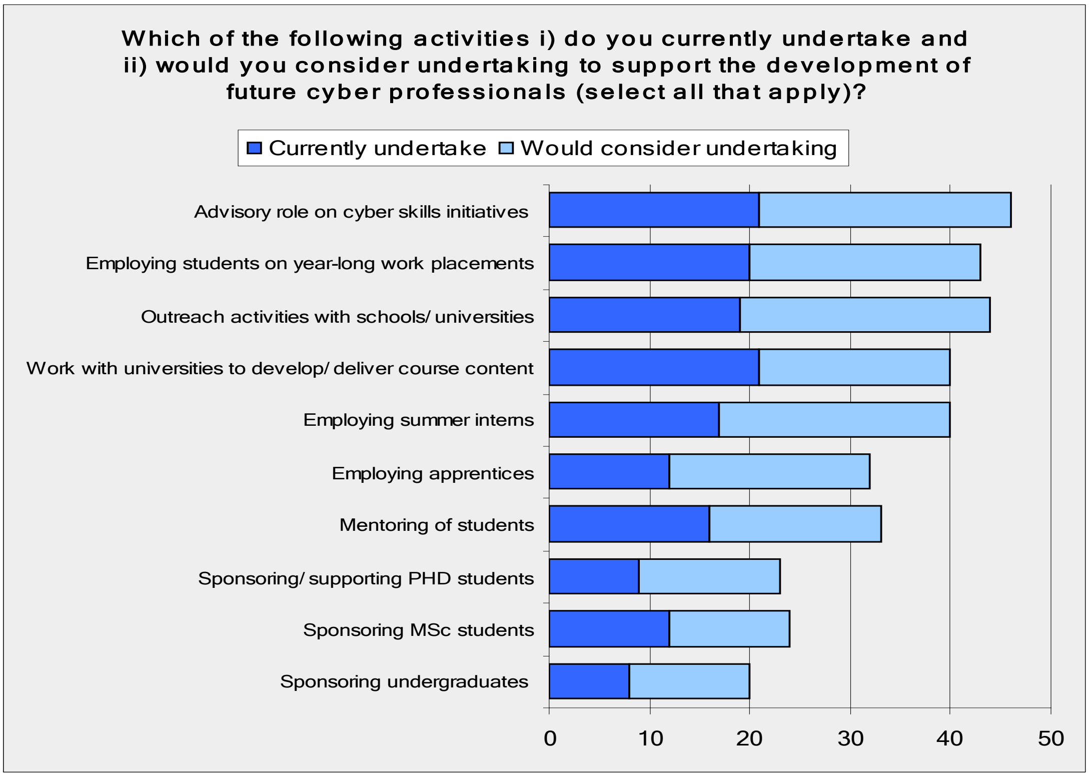


Chart 18:



Question 16: i) Are you aware of and ii) has your organisation participated in the following initiatives for which employer participation has been sought?

Question 17: If you are aware of, but have not participated in the initiatives referred to, what are the reasons for this?

Respondents had some awareness of the national activities that Government has funded over the last year (involving employers) but most had not participated for various reasons including short lead times or potentially having their own schemes. The greatest awareness was of the apprenticeship scheme (see chart 19). There were different issues with each scheme, lead in time was a problem for the IAAC cyber internship scheme, whilst cost was a barrier for the e-Skills UK cyber higher apprenticeship scheme (see chart 20). It should be noted that only a small proportion of respondents answered question 17.

Chart 19:

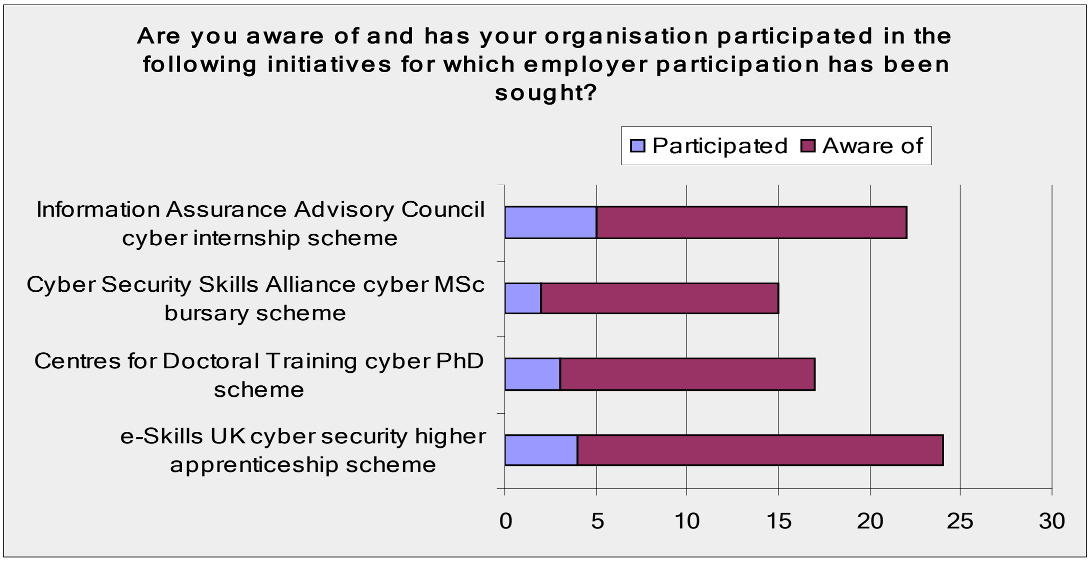
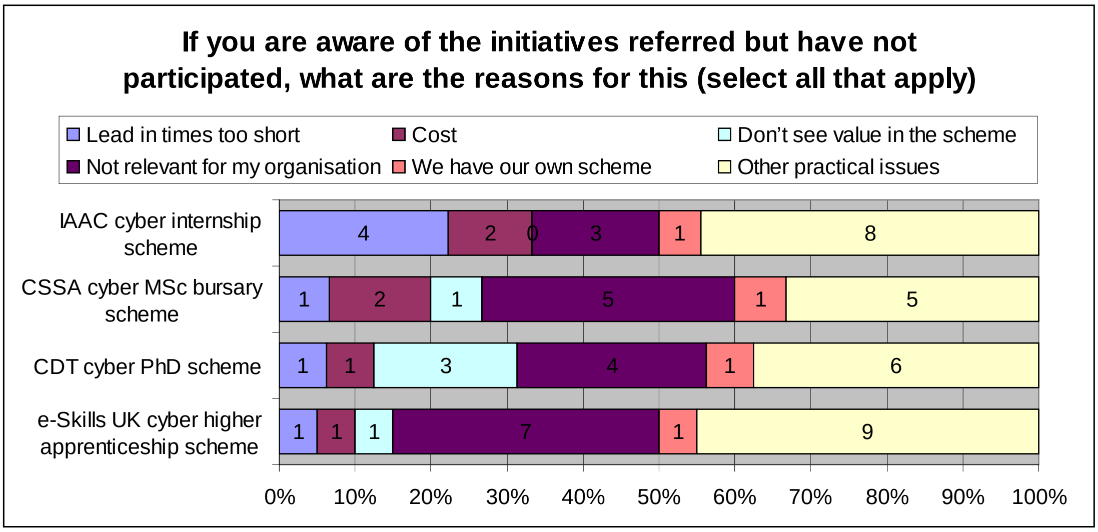


Chart 20:



Chapter 2: Workshop outputs

Discussion 1 – skills sources and shortages

a) What are your main skills shortages? Why?

Theme	Key point	Raised by
Specific skills shortages	Different technical skills shortages identified by different companies - security architects, security testers, general security operatives, customer facing consultants, experts in IA methodologies, incident responders, forensics, audit.	Primes
	Different technical skills shortages identified by different companies - sourcing and interpreting threat intelligence, Big Data Analysis (focusing on security events), Incident response professionals, security analysts, network security, penetration testers, CLAS consultants, SOC roles, PKI roles, malware reverse engineering	CNI
	Skills required to support development of security in emerging technologies and practices, e.g. mobile devices (telephone / tablet etc...), bring your own device, use of social media by businesses	CNI, Retail/Universities
	Shortage of soft skills (e.g. communication, team, creative thinking) and business skills/understanding. These are essential for explaining threat and solutions to Board/customers, delivering cultural change and for balancing business and security priorities. Some companies looked for these skills in their technical staff, whilst others had separate technical and business/client facing roles, depending on nature and size of business. Ability for people filling different roles to work as a team seen as essential.	Primes, CNI, SME, Retail/universities
	Recent graduates in particular often lack the soft and business skills required by recruiters.	Primes
	There is a shortage of software developers, programmers and computer engineers who understand cyber security – software, programming and	Primes, CNI, SME, Retail/Universities

Theme	Key point	Raised by
	infrastructure aren't safe by design.	
	Lack of understanding at Board level of cyber security threat, and the skill requirements for addressing it. This applies within public sector and private sector organisations.	Primes, CNI, SMEs, Retail/Universities
Underlying causes	Lack of awareness about cyber security as an attractive profession amongst potential recruits (both young people and potential career transitioners) and a lack of clearly articulated career pathways. This may put off girls in particular.	Primes, CNI, SMEs
	Teaching of computing in schools is too focused on applications with insufficient attention given to how computers work and information security and to fostering team skills.	Primes, CNI, SMEs
	Too few students, and too few girls in particular, are taking STEM subjects at school and university. Teaching of these subjects is focused towards boys, with the assumption that students will be male.	Primes, CNI, SMEs, Retail/Universities
	Undergraduate degrees may not adequately prepare students for the workplace – they often lack technical and soft skills, as well as work experience. Difficult for universities to keep up with the pace of change in cyber security and it was reported that some universities are not keen to engage with employers to discuss course content. Issue that students may rate courses perceived as 'difficult' less highly, discouraging universities from including cyber security content.	Primes, CNI, SME
	Recruitment pool limited by nationality – British nationals required for many roles.	Primes, SMEs
	Security clearance is perceived to be a barrier for SMEs wishing to recruit new or temporary staff. Security clearance needs to be obtained via a prime company, and can be time consuming and costly.	SMEs
	Various industries, many more established than cyber security, are competing for the same talent.	Primes, Retail/Universities
Recruitment and procurement practices	HR departments sometimes have limited understanding of the technical skills required for cyber roles, and can sift out candidates who don't have strong inter-personal skills but might be technically strong. Also, limited understanding of the professional qualifications that are relevant for particular	Primes, CNI, SME, Retail/Universities

Theme	Key point	Raised by
	roles.	
	Procurers of cyber security services sometimes don’t understand what skills/professional qualifications are required for the service they are buying, and may specify inappropriate requirements.	Primes, CNI, SME
Consequences of skills shortages	Salaries have become inflated as a result of competition for good staff.	Primes and Retail/Universities
	In some cases it is possible to recruit technical contractors, but can be difficult to fill permanent posts.	Primes, Retail/Universities
	Particularly difficult for small companies to retain staff because they cannot compete on salaries or prestige. They invest in staff training and development, only to lose them to bigger companies.	SMEs
	The workforce is getting older, lacking new blood and ideas.	CNI

b) What are your main skills sources?

Theme	Key point	Raised by
Recruitment practices	Recruitment often the result of recommendations and informal recruitment practices. Headhunting seems to be particularly common amongst CNI companies, given their preference for recruiting experienced professionals.	Primes, CNI
	Some CNI companies contract out most of their cyber security and employ very few staff in-house. They expect the suppliers of their cyber security services to ensure staff have appropriate skills. A few CNI companies have brought cyber security response in-house, upskilling their own staff and reducing reliance on external contractors/providers.	CNI
	Retail/Universities have cyber security staff based in IT departments or contract out most of their cyber security.	Retail/Universities
	It can be difficult for SMEs to know where to find potential talent, and to attract / pay for experienced professionals, particularly outside of London. There is therefore a focus on growing their own talent.	SMEs
Experienced professionals	Large companies (and CNI/retail companies in particular) tend to focus recruitment efforts on attracting experienced cyber security professionals rather than new graduates or career transitioners. It was mentioned that experience can be valued more highly than either academic or professional qualifications. It was recognised that this heavy reliance on experienced professionals is not sustainable – there needs to be a way for new entrants to the business to gain the experience they need to build a wider cadre of cyber professionals.	CNI, Retail/Universities
Career transitioners	A range of companies recruit from the Armed Forces (in particular), Security Services and the Police. Recruits valued for transferrable skills, foundation knowledge and work ethic.	Primes, CNI, SME
	A range of companies recruit experienced IT practitioners (either internally or externally) and train them up in cyber security.	Primes, CNI, Retail
Graduates	Whilst some companies do recruit graduates, they often require quite intensive training both in technical disciplines and in interpersonal and work-place skills. They have a lack of work experience. It can be difficult to place young recruits in certain roles, e.g. where significant interaction with clients or board members is required. Young recruits particularly valued for innovation/lateral thinking skills.	Primes, CNI
	Given difficulties recruiting experienced staff, SMEs more regularly employ graduates and provide them with significant one to one training and support.	SMEs
	Only a few companies said that they preferentially recruit graduates from cyber security	Primes, CNI, SME

Theme	Key point	Raised by
	degrees. Graduates were more commonly from other STEM subjects, or occasionally other disciplines (e.g. psychology, history)	
	Universities reported training up promising graduates from their own courses to fill cyber security roles.	Retail/Universities
	Masters degrees generally valued equally to undergraduate degrees (although there were exceptions to this) – comments that masters degrees were too theoretical. Doctorates can provide research skills and knowledge useful/essential in some businesses (particularly research-based organisations)	Primes, CNI, SME
Apprentices / school leavers	Some current use of apprentices (see discussion 2 for more details)	Primes, CNI SME
	Some SMEs recruit school leavers (informal apprentices), facilitated by strong outreach and work experience provision for local schools. School leavers valued for their technical abilities and innovation.	SME
Enthusiasts	Sometimes individuals with no relevant academic qualifications are recruited because of their enthusiasm and self-taught knowledge and skills	CNI, SME
Professional qualifications	Technical qualifications generally considered more useful than advanced-level academic study. CISSP is particularly in demand. IISP accreditation was also sought be some (and had not been included in the questionnaire options. It was recognised that the CCP scheme has helped to provide some clarify and assurance in relation to skill requirements for Government projects. However, Some mentioned that the array of qualifications and accreditations can be confusing and felt that there are too many. It can also be resource intensive for individuals/companies to maintain the range of accreditations/professional body memberships necessary to secure business.	Primes, CNI
	Value placed on some professional qualifications, e.g. CLAS partly because they are what clients are seeking, whether or not they represent the best qualification for the role.	SME

Discussion 2 – Business activity

a) What does your business currently do to support the development of your own cyber professionals?
e.g. graduate schemes, apprenticeships, training, CPD, mentoring

Theme	Key point	Raised by
Training and development	Some large companies have formal cyber graduate or new-entrant training programmes, up to 18 months in length, including lab-based and immersive training. One company has its own security academy with accredited learning pathways at different levels. Others have more ad hoc or personalised approaches to training new staff.	Primes, CNI
	CNI/Retail companies tend to buy-in external training where required rather than deliver their own, but focus is generally on recruiting staff who are already trained. Some companies referred to difficulty identifying which training is good and the expense of buying in external training.	CNI, Retail
	SMEs tend to take a very personalised and on-the-job approach to training, with time spent shadowing and learning from more experienced staff.	SME
	Mentoring common across range of organisations	Primes, SME
	CPD tends to be focused around individual needs, and is sometimes linked to securing or maintaining a range of professional qualifications and accreditations (e.g. CISSP, CLAS, CHECK). One company has a specific CLAS training programme. Some companies referred to supporting staff to access CPD through the IET, BCS, IISP and CREST.	Primes, CNI, Retail/Universities
Apprenticeships	Some companies already employ apprentices and in general they were seen as a valuable potential source of talent, and a way of embedding skills into companies. However, time and effort required to train, and won't be appropriate for all roles. Concern raised that both young people and their parents/teachers see apprenticeships as inferior to a standard university route at the moment. A formal higher apprenticeship scheme including a foundation degree (under development) was welcomed as a way of improving credibility and making it an easier option for employers. Some companies were involved in developing this scheme. Reference to "the 5% Club" where FTSE 350 organisations are being encouraged to support STEM Apprenticeships.	Primes, CNI, SMEs, Retail/Universities

b) What does your business currently do to support the development of the cyber workforce of the future?
e.g. internships, student sponsorship, work in schools, supporting universities to design/deliver courses

Theme	**Key point**	**Raised by**
Schools	Some companies involved with projects in local schools, e.g. through STEM Net. Example of collaboration between cyber prime and SME working together to offer extended work experience placements to local school children and undertake outreach work in schools to raise awareness about cyber security. Has increased interest in cyber security and resulted in permanent jobs in some cases.	Primes, SMEs
	Although there are some examples of company-wide outreach schemes with schools and universities (including in collaboration with the Welsh Government), most employees who get involved with this work do so of their own volition.	Primes
Higher education	Some companies have hosted interns or sandwich placements (some cyber-specific and some more generalist, with cyber element) and see value in internships as an extended recruitment tool as well as a way of giving students the work experience that companies are looking for. However, most companies don't employ interns at the moment – either they have not considered it at all, or have considered it but could not see the value for their organisation, or have been put off by bureaucracy, security clearance problems etc (see discussion 3 for more details). It was, however, recognised that there need to be more opportunities for students to gain work experience.	Primes, CNI
	A few companies sponsor individuals through university degrees	Primes, CNI
	A few companies are involved in the Cyber Security Centres for Doctoral Training, including sponsorship of PhD students.	Primes
	Some companies work with universities on the development and delivery of course content	Primes, CNI
Attracting new talent	Wide range of companies involved with sponsorship and delivery of the Cyber Security Challenge, and consider this a worthwhile programme as well as a useful recruitment tool.	Primes, CNI, SME
Diversity	Employees from some organizations involved in action to increase representation of women in cyber security.	Primes
National projects	Some companies provide input to national projects, e.g. through employer groups for e-Skills UK, BIS, GCHQ.	Primes

Discussion 3 – Government-supported interventions

a) Why do you think business take-up of the internships and masters bursary schemes, supported by Government, has been limited?
e.g. expense? Value to business? Lead in time? Other practical issues?

b) What factors are important in ensuring that any future internship/masters bursary schemes (and new initiatives on apprenticeships and centres for doctoral training), meet business needs?

Theme	**Key point**	**Raised by**
General reasons for limited take-up	Lack of awareness about these schemes, and information may have gone to the wrong people within organisations. There is perceived to be a lot of activity in the cyber security skills space, which can be confusing for businesses.	Primes, CNI, SMEs
	Schemes promoted individually rather than as part of a coherent wider skills strategy/jigsaw.	Primes
	Couldn't see immediate benefit to the business from participating in the schemes	Primes, CNI,
	Lack of priority given to cyber security by some Boards is reflected in a lack of engagement with cyber skills development. It is challenging to secure investment because it's an immature area, still working out what its needs are and how best to meet them.	CNI
	Some large companies said that if they wanted to take on interns or sponsor masters students they would arrange it themselves – Government didn't need to be involved.	Primes, CNI
	Some cyber teams don't have the time or money to support these schemes.	CNI, SMEs
Limited take up of internships	On internships – some thought lead-in times were too short (although others said the incubation time from idea to delivery was too long). Disconnect with corporate processes and business planning timetables.	Primes
	Some companies thought that summer internships are too short to be of use to the business	Primes, CNI
	Security clearance requirement for work in some companies perceived as a major hurdle to employing interns – getting security clearance is expensive and time consuming but without it the work options for interns are limited, and they may not be able to access physical work areas/IT systems. An uncleared intern could also pose a potential security risk (insider threat)	Primes, CNI, SMEs
Limited take up of masters bursaries	Insufficient broad demand for employees with cyber security MSc degrees to make a national sponsorship scheme viable.	Primes, CNI, SMEs
Increasing future take up	See chapter 3 for suggestions on increasing future take up	Primes, CNI, SMEs

Chapter 3: Business suggestions and Government Response

What more needs to be done to boost the capability of the cyber workforce today and the pipeline of future cyber talent

The tables below set out business suggestions, who the suggestions are for, where they were raised and the Government response (in blue).

Develop the workforce of the future and the workforce of today

Schools

Suggestion	For	Raised by
Cyber security, along with e-safety, should be embedded in the computing curriculum in primary and secondary schools and focused on girls as well as boys. This is an area where Government (as opposed to the market taking care of itself) can really add value. Teachers should receive support to help them teach children about cyber security, e.g. using e-Skills UK 'Behind the Screen' materials. Tools like Raspberry Pi computers should be used to teach children more about how computers work, rather than just how to use them.	Government	Cyber prime and SME, CNI, questionnaire
The computing curriculum has been changed to focus more on how computers work, rather than on applications. The changes which are being implemented in September 2014 will include a focus on programming and how to keep information safe. The Department for Education (DfE) is funding the British Computing SocietyBCS to provide support to teachers to implement all elements of the new computing curriculum, including aspects relevant to e-safety. This support includes the provision of £25,000 tax free scholarships for computer science trainee teachers who have the potential to become future school leaders (selected by top tech employers). The Network of Teaching Excellence in Computer Science (also funded by DfE) is recruiting 400 computer science Master Teachers, who will provide Continuing Professional Development to 16,000 teachers a year. This scheme is also backed by Microsoft and Google. To help lock cyber security into these broader developments the Government has funded the production of materials to enable schools to teach children about cyber security, and raise awareness of it as a potentially exciting career opportunity. The e-Skills UK teaching materials at key stage 4 and 5 (key stage 4 *Behind the Screen* will deliver 1 million hours of aggregate student learning in cyber security in at least 300 schools and key stage 5 materials will be available online shortly). Key stage 3 materials will be developed in 2014-15. In 2014-15 we also intend to fund e-skillsUK and NAACE to develop, accredit and deliver cyber security CPD for teachers, equipping them to include cyber security when teaching the new computing curriculum, and to make best use of complementary teaching and learning materials. Added to this e-skills UK will also roll out its Cyber Academy inspirational *Secure Futures* programme in London, Greater Manchester and Sussex following a successful pilot in Worcestershire. This, complemented by other exciting initiatives such as the Cyber		

Suggestion	For	Raised by
Security Challenge Schools Programme and the e-skills UK's award winning *Computer Club For Girls* programme (which is delivering "coding" courseware sponsored by business to 11-14 year old girls) has created multiple opportunities to support young people to learn how to be safe and secure in cyber space.		
Government and business need to collaborate on the promotion of STEM subjects in schools. Business involvement should help to raise awareness about cyber security as a career and build real-world credibility into teaching about cyber security.	Government Business	CNI, SME and Prime cyber, questionnaire
We are supportive of business working with schools to raise awareness of cyber security and *Cyber Security Skills: A guide for business* sets out the key options available for businesses wishing to do so. Opportunities supported by Government include the e-Skills *Secure Futures* programme and the Cyber Security Challenge Schools Programme mentioned above. The Department for Business, Innovation and Skills (BIS) also funds STEMNET to run the STEM Ambassadors programme, a nationwide network of over 27,000 DBS-checked volunteers from science, engineering and technical companies or academia, who work with schools across the UK. The STEM Ambassadors both raise awareness amongst children of the range of careers that science and technical qualifications offer and provide stimulating activities to increase their interest in STEM subjects. There are currently around 100 cyber STEM ambassadors, and we are keen to encourage more cyber professionals to take up this opportunity. 40% of STEM ambassadors are women. BIS also funds the National Science and Engineering Week which is a ten day (14 to 23 March 2014) programme of science, engineering and technology events and activities across the UK aimed at people of all ages. Last year it attracted about 1.6 million participants who took part in over 4,000 events across the country.		
Schools should be incentivised to encourage students to take STEM subjects at A level, e.g. by weighting them more highly in league tables to reflect greater difficulty	Government	CNI
We do not agree that STEM subjects are necessarily more difficult than others, and have no plans to weight them more highly in league tables. However, it is important to demonstrate to schools and pupils the value placed on STEM qualifications by employers (e.g. through the initiatives referred to above) and by universities (e.g. the Russell Group have provided a clear indication of those A level subjects that are most valued by universities (including STEM subjects) in their *Informed Choices* document).		

Apprenticeships

Suggestion	For	Raised by
Apprentices should provide a good source of talent for business. The new information security higher apprenticeship framework, incorporating a foundation degree, will make it easier for employers to recruit and train apprentices to HE-level along a vocational pathway. Training needs to meet business needs and training providers need to be in place to support such a scheme.	Business, Government, e-Skills UK	Cyber SME and Prime, CNI, questionnaire

Suggestion	**For**	**Raised by**
We welcome business support for the new employer-led cyber security higher apprenticeship scheme, delivered by e-skills UK and funded by UK Commision for Employment and Skills (UKCES). It has been designed by employers to ensure it meets business needs. The new SASE compliant cyber security apprenticeship frameworks have been published and employers are showing early interest in supporting the scheme. Details of how to get involved are provided in the *Cyber Security Skills: A guide for business.*		
Need to promote cyber security apprenticeships with young people (and their teachers/parents) as a credible alternative to a traditional university route (like the Rolls Royce scheme).	Government, e-Skills UK, Business	Cyber SME
We believe that higher apprenticeships are a credible alternative to a traditional university route. Marketing of the cyber security scheme to young people, and their teachers and parents will be an important element of the design and delivery process and e-skills UK is planning to launch a branded business programme to promote apprenticeships. More generally, the Apprenticeships Reform Implementation Plan launched 28 October 2013 set out our long term plan for growing the number of apprenticeships offered by employers by putting employers in the driving seat and giving them the opportunity to lead the way in developing and implementing new apprenticeships in their sectors. Trailblazers, led by employers and professional bodies will lead the way in implementing the new apprenticeships, and one has been established for the digital industries. The National Apprenticeships Service promotes apprenticeships through high-profile campaigns such as National Apprenticeship Week (3-7 March 2014) and provides a variety of toolkit and other resources for key stakeholders including employers and schools on the process and benefits of engagement.		
Should consider providing apprenticeships linked to professional qualifications.	Government, e-Skills UK	Questionnaire
The e-skills UK Cyber Security Higher Apprenticeship, which includes a City and Guilds Foundation Degree qualification, gives a broad foundation in cyber security. Once completed and achieved the participant has a good grounding to choose either a generalist or specialist cyber security career path which ultimately may lead to further relevant professional qualifications. Whether a professional qualification is appropriate, and if so, which qualification, should be a decision for the employer and individual. Subject to resources, e-skills UK plan to include such information on its Cyber Security Learning Pathways.		
Movement of funds from Training Providers to Business (as per the Richards Review) will be important for success of apprenticeships.	Government	Cyber prime
The Apprenticeship Reforms announced in October 2013 - are designed to give employers a greater say over the development of Apprenticeships in their sector and will put employers in the driving seat, ensuring that Apprenticeships deliver rigorous training that supports economic growth. We will simplify Apprenticeships replacing long and complex frameworks with new Apprenticeship standards of around one page written by employers in clear language that they understand. The movement of funds from Training Providers to employers will place control more firmly in the hands of employers, with every Apprenticeship based on rigorous business-set standards.		

Higher education

Suggestion	For	Raised by
Needs to be closer working between academia and business to a) make educators for all ICT/Computer Science courses aware of developments in cyber security and b) ensure that degree courses (undergraduate and masters) meet business needs. It would be useful for businesses to have some guidance on how to get involved with relevant universities. One option could be for educators to do placements in business. Suggestion that there should be a professional body for academics teaching cyber security.	Universities, Business	Cyber Primes and SME, CNI, questionnaire
These recommendations are primarily for business and academia. However, we are absolutely clear that we want businesses to engage with universities, both to support future employees - perhaps supporting them with sponsorship, helping to design provision and providing work experience. In 2014-15, we will fund the HE Academy to provide grants supporting the sort of cyber security teaching and learning developments employers call for, via its computing network. Universities will be encouraged to work with businesses on applications where relevant. In 2014-15 we will be working with delivery partners to develop a programme to identify different ways for computer science lecturers to spend time in business, e.g. through placements projects (including with cyber security companies where relevant). We have provided pump priming funding for the National Centre for Universities and Business (NCUB) which develops, promotes and supports world class collaboration between universities and businesses across the UK. NCUB is keen to engage with cyber networks and businesses as part of their plans to broker a closer and more sustainable relationship between business and universities. This will provide a coherent national platform for academia and business to work together on cyber education. GCHQ, supported by BIS and OCSIA are consulting extensively with academia and business to define a set of criteria which will identify those Universities that are excellent in the cyber security education (ACE-CSE) they provide. This initiative is intended to complement the current Academic Centres of Excellence in Cyber Security Research (ACE-CSRs). Recognising such universities will allow GCHQ and other employers to easily identify those institutions delivering quality education in cyber security. As a an initial step in the ACE-CSE programme, GCHQ intends to first identify high quality Masters courses through a new certification scheme focused specifically on the various elements of cyber security.		
Should consider including professional cyber qualification as part of undergraduate or masters degree (but work experience would need to be essential component in order to demonstrate competence)	Universities	Cyber SME
Some universities already provide degrees which include or strongly link to a professional qualification, for example University of Lancaster and De Montfort University Leicester. It is also possible to gain credits towards elements of Open University degrees with a relevant vendor qualification in lieu of academic study. BIS is exploring how the NCSP can work with the HE Academy to widen established interest within the computing discipline in making use of vendor resources and vendor-specific certification to enhance curricula and graduate employability. This would enable us to support course developments in the field of cyber security specifically but also across computing more generally.		
Cyber security should be embedded in all computer science and software engineering courses and qualifications.	IET and BCS, Universities,	All workshops

Suggestion	For	Raised by
	supported by Government	
From 2016 all university courses to be accredited by the Institution of Engineering and Technology (IET) and the British Computing Society (BCS) (including the vast majority of computer science, computing and software engineering degrees) will be required to deliver mandatory learning outcomes on information security (courses accredited by the BCS already include information security learning outcomes). All engineers and IT professionals registering with the IET and BCS will also be required to demonstrate an awareness of information security. This will be underpinned by the inclusion of ‘security’ in the UK Standard for Professional Engineering Competence (UKSPEC) from 2014, with implications for learning outcomes and registration requirements across the engineering profession. To support universities to deliver these learning outcomes, the Trusted Software Initiative (TSI) has received funding under the NCSP to develop learning materials on developing safe and secure software that universities can use free of charge.		
More students should be encouraged to take undergraduate courses relevant to cyber security, e.g. through reduced fees for relevant courses	Government	Questionnaire
Universities are private organisations which can attract public funding. Independence and autonomy is the defining characteristic of UK Higher Education Institutions and autonomy means letting the universities set their own mission and develop their own curriculum. It is not for Government to prescribe what people study or limit the subjects’ colleges and universities offer. As part of our Higher Education reforms, universities will fund their courses through the income they receive from tuition charges – as well as any additional investment they secure – so the university funding flows from student choice. We are asking every institution to provide prospective students with clear and comparable information about, for example, course content, teaching methods and crucially the employment outcomes of previous students. A ‘Key Information Set’, comprising the items of information that students have said they want, should be published on each university website on a course by course basis. We also plan to build on the existing Unistats website to ensure that information is readily available to enable students and businesses to better evaluate computer science (including cyber security) courses. Existing NCSP activity such as through the Cyber Academy and Cyber Security Challenge schools outreach work is also helping to raise young people’s awareness of careers - and of higher education as one important pathway towards future employment - in this area.		
If students are to gain the work experience they need to ensure they have the right skills for the workplace, businesses need to provide opportunities for mentored work experience/internships/sandwich placements. These should be flexible in length – longer placements will often be of most benefit to the company. For their part, universities should encourage students to undertake internships of work placements within their degree.	Business, supported by Universities, Government, e-Skills UK	All workshops and questionnaire
This suggestion is primarily for business and universities. However, we are supportive of business providing work experience opportunities for students, and recognise the benefits a business can derive from hosting a talented intern. The e-Skills UK Cyber Security Internship scheme, funded by Government, will facilitate the provision of business internship placements of varying lengths for students during or after their degrees. A supporting website for the scheme is now live. More information on how employers can get involved with the internship scheme can be found in *Cyber Security Skills: A guide for business.*		

Suggestion	For	Raised by
We agree that internships of various lengths might best meet the diverse range of employer needs and circumstances. e-skills UK recommended a minimum of three months to a maximum of twelve months. As part of the ACE CSE certification process, GCHQ will explore an element of work placement as part of the criteria for a future certified Bachelors in cyber security.		
Need to overcome problems of security clearance requirements where these arise to enable more internships.	Government	CNI, Cyber SMEs
We are aware that security clearance may be an issue for some companies working on particularly sensitive contracts. However, feedback from those involved in cyber security internship schemes is that internship opportunities can in practice be conveniently shaped and controlled so as to ensure students have access to appropriate areas of work that both benefit their development and the employer's day-to-day business. Existing providers of internships have shown it is possible to offer controlled yet valuable exposure to real-world cyber security issues, with some businesses accordingly being comfortable to use only a baseline security clearance.		
There is unlikely to be a need for an ongoing business masters bursary scheme at the present time. If companies wish to sponsor masters (or undergraduate) students they should do so independently.	CSSA, Government, Business	Cyber Primes and SMEs, CNI
In 2013, the CSSA, supported by NCSP funding, piloted a bursary scheme for employers to fund promising students to undertake cyber security Masters degrees. Initial consultation with business suggested that there was likely to be business demand for such a scheme. However the result of the pilot concluded that although Masters degrees provide a pathway to a cyber profession, there is insufficient employer demand for a central scheme. Whilst the advanced level education offered by a cyber security Masters degree can have benefits for both students and employers, sponsorship can be arranged independently where appropriate. To coincide with the launch of the ACE CSE Masters in Cyber Security in September 2014, GCHQ will explore the opportunity for a public sector post graduate bursary.		

Attracting people into the cyber profession

Recommendation	For	Raised by
Need to increase awareness of cyber security sector as a ‘profession’ with an attractive career path, capitalising on the fact that ‘geeks are now cool’. Should establish and publicise clear learning and career pathways to school pupils, university students and professionals from related disciplines. Consider how gamification and media (e.g. cyber security documentary) could be used to attract people into cyber.	Business Government Professional Bodies e-Skills/Cyber Security Challenge	All workshops and questionnaire
This is the responsibility of all the parties referred to. Encouraging people to join the profession is a key part of developing a vibrant and self-sustaining community of cyber and information security specialists. We are involved in the following interventions to encourage more people into cyber security such as: • Funding a range of inspiring activity in schools (see schools section). • Funding e-Skills UK, working with GCHQ, IISP and employers, to align skills standards in Cyber Security and build learning pathways which are aligned to selected roles within the CESG Certified Professional (CCP) scheme. • Funding CREST to develop on-line resources to help illuminate routes towards a wide range of cyber security roles • Sponsorship of the Cyber Security Challenge and the National Cipher Challenge, which use gamification to attract students and existing professionals into cyber security. • Funded ‘Graduate Prospects’ to develop within their careers site a page drawing student and recent graduate attention to career opportunities within cyber security • Providing advice for business on how they can get involved in these interventions through *Cyber Security Skills: A guide for business*		
Career transition programmes, e.g. from military/IT should be established	Training Providers/ Business/with government assistance	Cyber Primes, questionnaire
OCSIA and MOD are keen supporters of the CompTIA ‘Armed for IT’ initiative which is focused on getting service leavers into information technology and cyber security careers.		
It would be useful (for SMEs in particular) to have business-wide recruitment events, where potential candidates can meet employers.	Recruitment consultants, trade associations, universities?	Cyber SMEs

Recommendation	For	Raised by
The Government has passed this recommendation on to relevant recruitment consultants and trade associations. On the basis of responses, we expect that a number of cyber security recruitment events will take place in 2014-15.		
Strong support for the Cyber Security Challenge. Competitions like this seen as crucial for attracting more people into cyber roles. Would support challenges aimed specifically at generating interest/enthusiasm amongst university students.	Government, Cyber Security Challenge, business	Cyber Primes and SMEs, CNI, questionnaire
We are providing funding to support the attraction of new talent and interest into cyber security through competitions such as the Cyber Security Challenge and National Cipher Challenge.These provide opportunities, advice and support for those looking to enter into the cyber security profession. Since its launch in 2010, the Challenge has had more than 10,000 registrations and received support from over 50 business sponsors. This year, the challenge introduced new competitions for schools in partnership with universities and businesses.		
Enabling secondments between business and GCHQ could help to broaden the experience of individuals and help to address recruitment and retention issues for GCHQ.	Government, Business	Cyber SMEs
GCHQ has a very limited and discrete secondment programme with trusted business partners. There are no current plans to increase the scale of this programme. However, there may be secondment opportunities for business with particular parts of government as more and more government / citizen transaction services are moved online.		
Companies (particularly SMEs), should be incentivised to grow cyber security talent e.g. through supporting the costs of internships or tax breaks for recruiting graduates.	Government	Retail/ Universities, CNI, Cyber SMEs
In general, we do not think it is appropriate for the Government to subsidise the costs of developing staff, including interns and new graduates. We believe that the benefits to employers of supporting new talent should make this a worthwhile investment for businesses. The evidence from the IAAC 2013 internship pilot scheme was that there was no widespread reluctance by providers of placements to cover payments to interns, particularly where the opportunity to host a student was considered well in advance and the student and business were well-matched.		

Develop a Cyber Profession

Professional qualifications

Recommendation	For	Raised by
CESG Certified Professional (CCP) scheme, currently focussed on Government systems, could be expanded as a nationally recognised scheme for business and local government.	Government	Questionnaire
GCHQ has established a new certification scheme for information assurance specialists, known as CESG Certified Professional (CCP). The six skills profiles associated with the current CCP roles focus, based on the IISP skills framework, primarily, although not exclusively, on the public sector. However, the scheme is now available to UK business and GCHQ is actively seeking business views on additional roles, the first of which will be the CCP Penetration Tester role in March 2014.		
Should consider whether the number of professional qualifications could be rationalised, although recognise that these are mostly business-led. It would be useful to have guidance on which professional qualifications and training courses are appropriate for different purposes, and which ones are rated most highly.	Government, Business	CNI, Cyber SMEs
The majority of cyber security professional qualifications and accreditations are owned by business and sustained by business demand. We cannot control how many qualifications and accreditations are brought to market, but through the CCP scheme we have developed the Government's approved standard for UK cyber security professionals, and made the scheme available to businesses who would like to use it. By working with business, academia and professional bodies, GCHQ also continues to broaden its range of certified standards in UK cyber security for people, products and services, to help individuals and businesses make informed decisions. In support of the CCP scheme, GCHQ is developing a process to accredit private sector training which supports cyber security professionals to gain the skills needed within the CCP Scheme. This provides a level of confidence to course attendees and employers that the cyber security subject material and the teaching are at an approved level. Relevant courses accredited under this process will be eligible to be showcased on e-skills UK's Cyber Academy Learning Pathways.		
There should be greater consistency in the standards applied by the different bodies operating the CCP scheme	GCHQ	CNI
When setting up the CCP scheme, CESG were primarily concerned with having a consistent outcome to the evidence submitted rather than prescribing the process the three certifying bodies should take for assessing the evidence. All three certifying bodies successfully passed a stringent CESG audit in 2013 which provides further confidence in the integrity of the CCP scheme.		
There should be a cyber qualification which people have to get to be a cyber security professional, consistent with other industries such as law, engineering.	Government, Professional bodies	CNI
CCP is the Government's approved standard for UK cyber security professionals. Over time, the scheme will evolve to include an ever broadening range of skills to meet UK government and business needs. GCHQ will also work with interested parties, including the Cyber Growth Partnership, wider business and professional bodies to explore the demand for a 'chartered' status.		

Recommendation	For	Raised by
Professional qualifications should lapse unless an individual shows that they are up to date with skills and knowledge.	Owners of professional qualifications	CNI
In order to be regarded as a CESG Certified Professional, applicants are required to re-submit evidence of applying cyber security skills and knowledge in a working environment every 3 years. Failure to renew their application will result in the loss of CCP certification. The renewal of other professional qualifications is a matter for the owners of the qualifications.		

Influence Associated Professions and the wider workforce

Recommendation	For	Raised by
Need to improve company boards' skills in understanding and managing cyber risks e.g. through including cyber security in MBAs, training for Company Secretaries and Directors. This would build on the positive start made by the 10 Steps guide and Cyber Governance Health Check.	Government, business	All workshops and questionnaire
BIS will work with the audit community again to repeat the Cyber Governance Health Check Tracker in 2014. A repeat Tracker would reinforce the existence of the risk, and indicate what measures boards can undertake to show leadership in risk mitigation. We will also use the Health Check as a route for promoting *Cyber Security Skills: A guide for business.* BIS will develop specific guidance for the investor community, providing them with key questions to ask boards, including references to skills and training. BIS and private sector partners will develop specific guidance for Non-Executive Directors (NEDs) and for inclusion in NED training packs and journals, which will enable NEDs to confidently and constructively challenge board colleagues on issues such as skills, culture, risk management. Government also provides cyber security and information assurance training to Non-Executive Directors (NEDs) and Board Members throughout the public sector, funded by the NCSP. We are aware of, and welcome efforts from a number of universities, working with businesses, to include cyber security in MBAs.		
All staff, particularly in high threat organisations should have a basic understanding of cyber security and the need to protect information – it shouldn't just be seen as an IT problem – we need cultural change. Cyber security should be included in the induction programmes for new entrants. Could be delivered through a MOOC.	Business, Government	CNI, Retail/Universitie s
We agree that all organisations should ensure that their staff have a basic understanding of cyber security and the need to protect information. This is primarily the responsibility of employers. All public sector staff are required to undertake a 'Responsible for Information' e-learning course. This course is being adapted to provide a training resource for the use of private sector organisations and in particular SMEs who may not have their own in-house training. The Government is also funding the Open University to develop an 'Introduction to Cyber' MOOC (Massive Open Online Course). The MOOC will make knowledge of cyber security more accessible across the board and provide a basic understanding of cyber security to participants, including those from		

Recommendation	For	Raised by
businesses. We will work with our academic and business stakeholders to encourage uptake of the course.		
Procurement departments in Government and the private sector need to be educated about how cyber security should be factored into IT and other relevant contracts, and the professional or academic qualifications that those providing cyber security services should have. Some argued that specific professional or academic qualifications should be a mandatory element of contracts.	Government, CIPS	Cyber Prime and SME, CNI
GCHQ is working with the ADPG (Aerospace and Defence Procurement Group) through CIPS (Chartered Institute of Purchasing and Supply) to improve cyber security procurement practices across their member organisations. A tiger team has been set up with the aim of driving forward a pan-industry approach to managing information risk particularly within the supply chains. As part of this work, GCHQ intends to host a briefing event for senior procurement professionals.		
Business need to educate recruitment firms and HR departments on the skills they are looking for	Business	Cyber Prime and SME, CNI
This recommendation is for business.		
CNI regulators should require organisations within their sector to demonstrate that they have appropriate cyber security skills within their organisation.	Government/ CNI Regulators	CNI
We have been working closely with regulators in the CNI sectors to help them identify and manage cyber risk in each sector. On 5 February, 2014, Secretary of State, Business, Innovation & Skills hosted a meeting with senior regulators, lead Government departments and the Security Services on ‘strengthening the cyber security of our essential services.’ A communiqué was issued following the event, outlining how Government and regulators will ‘embed cyber security in the firms and markets that they oversee.’ As the Government has noted previously, cyber risk is a business risk for companies, and needs be managed appropriately. All sectors will need to develop their skills and capabilities to effectively manage cyber risk as a business risk.		

Increase Cyber Security Research

Recommendation	**For**	**Raised by**
Funding under the CDT scheme should be open to part time as well as full time students to encourage professionals working in business (who have a lot of experience to offer) to undertake PhDs. CDT team should be focused on developing ‘researching professionals’, not ‘professional researchers’.	Government, CDTs	CNI
Funding for the CDT scheme is administered through EPSRC, part of Research Council UK, in line with Research Council funding guidelines. Part time students are also able to access funding to support their studies through Research Council funding.		

Manage, understand and promote

Recommendation	For	Raised by
There needs to be strong leadership within Government to deliver change in this area. Government interventions should be part of a coherent strategy to boost cyber security skills, and should be presented as such, not as stand-alone initiatives.	Government e-Skills UK	Cyber prime and questionnaire
Objective 4 of the National Cyber Security Strategy sets out our high level strategy on skills which has been delivered though a skills plan bringing together activities by BIS, Cabinet Office and GCHQ. There are interventions at every level of the education system and we have presented widely on our overall strategy. The present report provides up-to-date information on the range of interventions underway and planned for the future under our joint "skills plan". *Cyber Security Skills: A guide for business* explains how business can get involved. Ministers and senior officials within Cabinet Office, BIS and GCHQ are highly committed to delivering change on cyber security skills, as evidenced by the investment of time and resources in this agenda. We are committed to working closely with key strategic partners across the cyber security skills agenda to maximise impact and avoid duplication. Business also needs to show leadership in this area, and we welcome the efforts of the Cyber Growth Partnership to increase cyber security skills.		
Need to get the need for cyber security skills embedded into related strategies, e.g. Information Economy Strategy, London Business Crime Strategy	Government	Retail/ Universities
Cyber security does not exist in a vacuum and we will continue to work across Government and with partners to ensure that the importance of cyber security skills and capability is reflected and embedded in relevant strategies and plans, for example, in relation to the wider Information Economy or business crime.		
Need early and continuing engagement with business on design, delivery and evaluation – apprenticeship scheme is good model.	Government e-Skills UK Business	Cyber Prime and SME
Engagement with business has been, and will continue to be, central to the initiatives supported by Government. In the case of the e-skills UK Cyber Academy Higher Apprenticeship scheme, the critical success factor is end to end engagement of a relevant and passionate cohort of employers involved from initial design of learning outcomes to meet their needs through to delivery. Similarly, GCHQ has an employer advisory group which it consults closely on all GCHQ-led skills initiatives affecting business. The Information Assurance Advisory Council (IAAC) and the Cyber Security Skills Alliance (CSSA) have also consulted with business before launching key initiatives such as the internship and masters bursary pilots, and there is significant industry involvement in the delivery and evaluation of the schemes. Negotiation of relevant NCSP grants/contracts for 2014-15 skills and education activity will highlight the importance of engaging with business on design, development and delivery of interventions. In addition to the above employer engagement avenues, Government works very closely with Tech UK and the Cyber Growth Partnership who provide useful routes for consulting with the cyber security supplier sector.		
Need to promote skills interventions to employers widely, but in a targeted way: -Not all schemes will be right for all companies, e.g. larger companies may have their own schemes/smaller companies may not have the capacity to participate. -Could target companies who identify cyber as a 'top 10 risk' as may be more open to engaging in skills interventions. -Should use CPNI to promote skills interventions.	Government e-Skills UK Business	All workshops

Recommendation	For	Raised by
-Should encourage large companies to promote skills interventions with supply chain.		
Cyber Security Skills: A guide for business will be updated regularly and promoted through the following wide-ranging routes: • The Cyber Skills Reception and Showcase event • Key groups such as the Cyber Growth Partnership (CGP), Defence Cyber Protection Partnership (DCPP) and the Information Economy (IE) Council • Relevant trade associations (e.g. Tech UK), professional bodies (e.g. IET and BCS) and skills organisations (e.g. e-Skills UK, Cyber Security Challenge) • CPNI Information Exchanges • 2014-15 FTSE 350 tracker survey process • BIS partnerships such as with the retail sector. • Promotion by Government and its partners at external conferences and events • Encouraging providers and customers of cyber suppliers to get involved in interventions down the supply chain. Additionally, partners delivering specific initiatives will undertake their own marketing as appropriate.		
Need clear articulation of benefits for companies, supported by case studies, success stories etc. This needs to sell the benefits to Boards in business terms, not just appeal to security teams.	Government e-Skills UK Business	Cyber prime and SME, CNI
Cyber Security Skills: A guide for business (and associated promotion) will set out the key benefits for business involvement in Government-supported interventions including helping them to develop their own cyber workforce and the workforce of the future. Articulating business benefits has enabled organisations like e-Skills UK and the Cyber Security Challenge to secure business support for a range of initiatives. Our skills-focused messaging builds upon and benefits from broader business-focused messaging across the NCSP (e.g. in relation to board-level governance and organisational standards).		
Need longer lead-in times mapped to business planning cycles, but also important that companies can move quickly once they decide to get involved and see quick benefits.	Government e-Skills UK	Cyber prime
Where practicable, we and our delivery partners will take account of the impact of business planning cycles in the anticipated design and delivery timetables for relevant interventions. e-skills UK's approach to strategy and delivery is cognisant of the need for not only "quick wins" to keep business engaged but also a long term sustainable plan for each relevant activity which is commensurate with business cycles.		
Government should report back to business on the impact of different schemes.	Government e-Skills UK	Cyber prime
Together with our delivery partners, we will continue to make business aware of progress with and outcomes of the different schemes through the routes identified above.		

This publication is also available on our website at www.bis.gov.uk
Any enquiries regarding this publication should be sent to:

Department for Business, Innovation and Skills
1 Victoria Street
London SW1H 0ET
Tel: 020 7215 5000

If you require this publication in an alternative format, email enquiries@bis.gsi.gov.uk, or call 020 7215 5000.

BIS/14/648