HM Government

Cyber Security Skills

Business perspectives and Government's next steps

March 2014

Contents

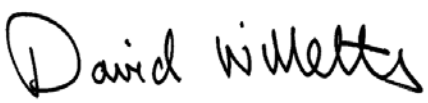
Foreword

This Government has a vision for a vibrant, resilient and secure cyberspace, contributing to economic prosperity, national security and a strong society. This vision can only become a reality if we have a strong cyber security skills base in the UK, both within Government and the private sector.

Whilst managing the threat posed by cyber attack presents businesses with challenges, it also provides opportunities. Having the skills and capability to manage cyber risk effectively can reduce the financial cost to a business from cyber crime, and it can also increase consumer confidence, providing that business with a competitive edge. As businesses increasingly take steps to protect themselves from cyber attack, demand for cyber security products and services will continue to increase, providing growth opportunities for the organisations that supply them. A highly skilled workforce will enable cyber suppliers to derive maximum benefit from these opportunities.

It is clearly in the interests of both businesses and Government to provide leadership and investment in this area. This is why we have engaged with businesses to ensure that our plans for increasing the UK's cyber security skills and capability continue to be informed by the challenges they face. I hope that businesses will join us, and our other delivery partners, in supporting these plans. Getting involved with the activities described in *Cyber Security Skills: A guide for business* is a good place to start.

I am very grateful for the time and expertise contributed by businesses to our engagement exercise, and to partners from Tech UK, e-skills UK, the Institution of Engineering and Technology and Malvern Cyber Security Cluster for their practical support.



David Willetts
Minister for Universities and Science

Executive Summary

Objective 4 of the UK's National Cyber Security Strategy is for the UK to have the cross-cutting knowledge, skills and capability it needs to deliver the wider Strategy. Through the National Cyber Security Programme (NCSP) the Department for Business Innovation and Skills (BIS), Government Communications Headquarters (GCHQ) and the Cabinet Office have partnered to lead and support activity to increase cyber security skills at all levels of education, and amongst the cyber security workforce over the past 2 and a half years. This work has been taken forward in close collaboration with business and the education and skills sectors. Significant progress has been made, for example:

- We have funded innovative activities and teaching materials to promote cyber security learning in schools and exciting competitions to attract people into the profession;
- We have funded initiatives for graduate and post graduate students, as well as internship and apprenticeship initiatives to strengthen the skills of entrants to the profession;
- We have accredited 11 universities as Academic Centres of Excellence in Cyber Security Research, set up 3 new Research Institutes and funded 2 Centres for Doctoral Training to develop high-end skills and capability; and
- We have strengthened the cyber security profession through the introduction of CESG's[1] Certified Professional scheme, and the development of National Skills Standards and learning pathways.

However, the cyber security landscape is constantly evolving and it is important to ensure we remain focussed on the right areas to build the foundations for long term transformational change.

Business engagement exercise

In late 2013 we therefore undertook a business engagement exercise aimed at ensuring that the cyber security skills activities we support continue to meet the needs of businesses. We were also keen to understand more about employer engagement with some of the national activities that Government has funded over the last year where translating initial business interest into commitments of support has been challenging.

The exercise 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. We received 81 responses to our questionnaire and held workshops with 51 individuals from a range of businesses, including those that employ cyber security professionals because they face a significant cyber threat and those that supply cyber security products and services.

[1] UK Government's National Technical Authority for Information Assurance

Key findings

The exercise highlighted a demand amongst businesses for more professionals with a range of technical skills, but also a demand for new entrants with stronger business skills and greater work experience. A range of reasons for the skills shortage were suggested, including the immaturity of cyber security as a 'profession', low take-up of STEM (Science, Technology, Engineering and Maths) subjects and limited awareness of cyber security as an interesting and rewarding career at all levels of the education system, and difficulty attracting female candidates. The exercise also highlighted the importance of increasing cyber skills amongst those who create, purchase and use technology to reduce business vulnerability to cyber attack, and amongst company decision makers who are responsible for managing business risks.

Most cyber security recruitment is UK-based and focused on experienced professionals, particularly outside the supplier sector. It was noted that businesses generally value experience more than either academic or professional qualifications. Given increasing demand, it was recognised that businesses need to provide more opportunities for individuals to gain that experience, for example, through internships and apprenticeships. There was a willingness to work with universities to increase cyber security content in relevant degree courses, and ensure that it meets employer needs. Finally, businesses were keen to collaborate with Government and other partners to encourage more young people, and those in other professions, to explore cyber security careers. To support this, it is important that cyber security is seen as a 'profession' with clear career pathways.

Future plans for NCSP skills activity

In 2014-15 we will be working with our delivery partners to support a programme of new and continuing activity to strengthen the supply of cyber security skills in the UK, informed by the suggestions made during our business engagement exercise. Our plans are closely aligned to, and benefit from a range of wider Government work, including efforts to strengthen digital skills across the information economy. A summary of key activities is set out below.

Develop the workforce of the future and the workforce of today

- We will continue to support activity in schools, for example, by e-skills UK, the Cyber Security Challenge and STEMNET, to raise awareness about cyber security careers, encourage take-up of technology-related subjects and educate students to be effective members of the broader digital economy.

- We will support universities, through the Higher Education Academy, to further innovation in cyber security teaching, and accredit Academic Centres of Excellence for Cyber Security Education, certifying high quality cyber security MSc courses as the first step in this process. Building on lessons learnt from pilot projects we will support e-skills UK to facilitate industry internships, helping meet business demand for individuals with experience. And we will support professional bodies, working with the Trustworthy Software initiative and universities, to embed cyber security into a range of software engineering and computing degrees.

- We will support alternative routes into cyber security careers through the new e-skills UK employer-led Cyber Security Apprenticeships and the Security and Intelligence Agencies Higher Apprenticeship Scheme, and explore other opportunities for vocational education and training in cyber security.

- We will attract students and existing professionals from wider fields into cyber security, for example through the Cyber Security Challenge and National Cipher Challenge, and inclusion of cyber security in a national campaign to communicate the range of exciting digital careers. We will continue to work with the Women's Security Society to advance women working in, or moving to, cyber security and ensure that diversity issues are considered as part of all our activities.

Develop a Cyber Profession

- We will continue to work with partners to put in place the building blocks for a cyber security profession, for example by expanding the CESG Certified Professional (CCP) scheme to ensure it meets the needs of businesses as well as the public sector, and accrediting private sector training which supports development of the skills needed for CCP accreditation. We will continue to support e-skills UK to develop learning pathways and skills standards in cyber security, mapped against the Institute of Information Security Professionals (IISP) skills framework and selected CCP roles, helping current and future cyber security professionals develop and manage their careers effectively.

Influence Associated Professions and the Wider Workforce

- We will work with businesses to increase board-level understanding of cyber security, for example through repeating the Cyber Governance Health Check Tracker, continuing to market the 10 Steps guidance, developing guidance for investors and non-executive directors in the private sector and delivering face to face training for non-executive directors in the public sector. We will support the development of cyber awareness training for the wider workforce, for example, through an 'Introduction to Cyber' MOOC (Massive Open Online Course) and 'Responsible for Information' e-learning for the use of small businesses.

- We will work with our partners, including relevant professional bodies, to increase the cyber security awareness of the IT, procurement, legal, accountancy and audit professions through supporting guidance, training and events.

Increase cyber security research

- We will build a cutting edge research capability to increase high-end cyber security skills and ensure a strong UK knowledge base, through continuing to support 3 Research Institutes, 2 Centres for Doctoral Training and 11 Academic Centres of Excellence for Cyber Security Research (another call for ACE CSRs will go out this year).

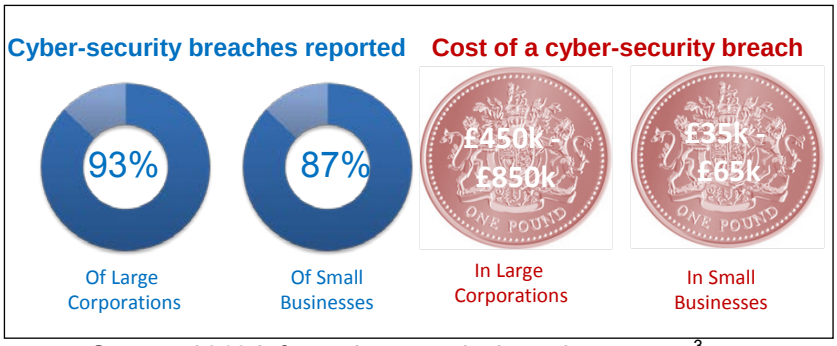
Conclusion

It is important not to underestimate the scale of the challenge that faces the UK in securing the skills required to meet increasing demand. Working in partnership across Government, business and the education and skills sectors we have already made significant progress. Strong business leadership is becoming increasingly important as we seek to embed cyber security skills more deeply in the fabric of organisations, and strengthen the pipeline of future talent. Many businesses are already showing this leadership, and others are keen to do so, recognising the benefits this offers to their organisation. Our new *Cyber Security Skills: A guide for business* will help them to identify excellent practical opportunities to support the development of cyber security skills.

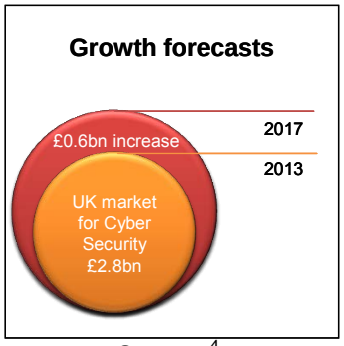
Chapter 1: Introduction

1.1 Our vision, set out in the National Cyber Security Strategy (NCSS), is for the UK to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society. Objective 4 of the strategy is for the UK to have the cross-cutting knowledge, skills and capability it needs to deliver this vision by extending knowledge and enhancing skills.

1.2 This is a challenging objective, and not just for the UK. The Global Information Security Workforce Study by Frost and Sullivan consultants found that the global demand for people with cyber security skills is forecast to grow at about 13.2% each year from 2012 to 2017[2]. The National Audit Office Landscape Review on the UK Cyber Security Strategy, published in February 2013, identified a shortage of cyber security skills as a key challenge. The Review concluded that the current pipeline of graduates and practitioners would not meet growing demand. This has implications for UK resilience, but also for economic growth. The *Competitive analysis of the UK cyber security sector* produced by Pierre Audoin Consultants on behalf of BIS in July 2013 identified the availability of skills as a key barrier to growth of the cyber security sector. Creating future generations of highly-skilled cyber specialists and cyber-aware professionals will help ensure that the UK is well positioned to respond to the cyber threats it faces. It will also allow the UK to reap the economic benefits derived from reducing security breaches and growth in the cyber security sector.



Source: 2013 Information security breaches survey[3]

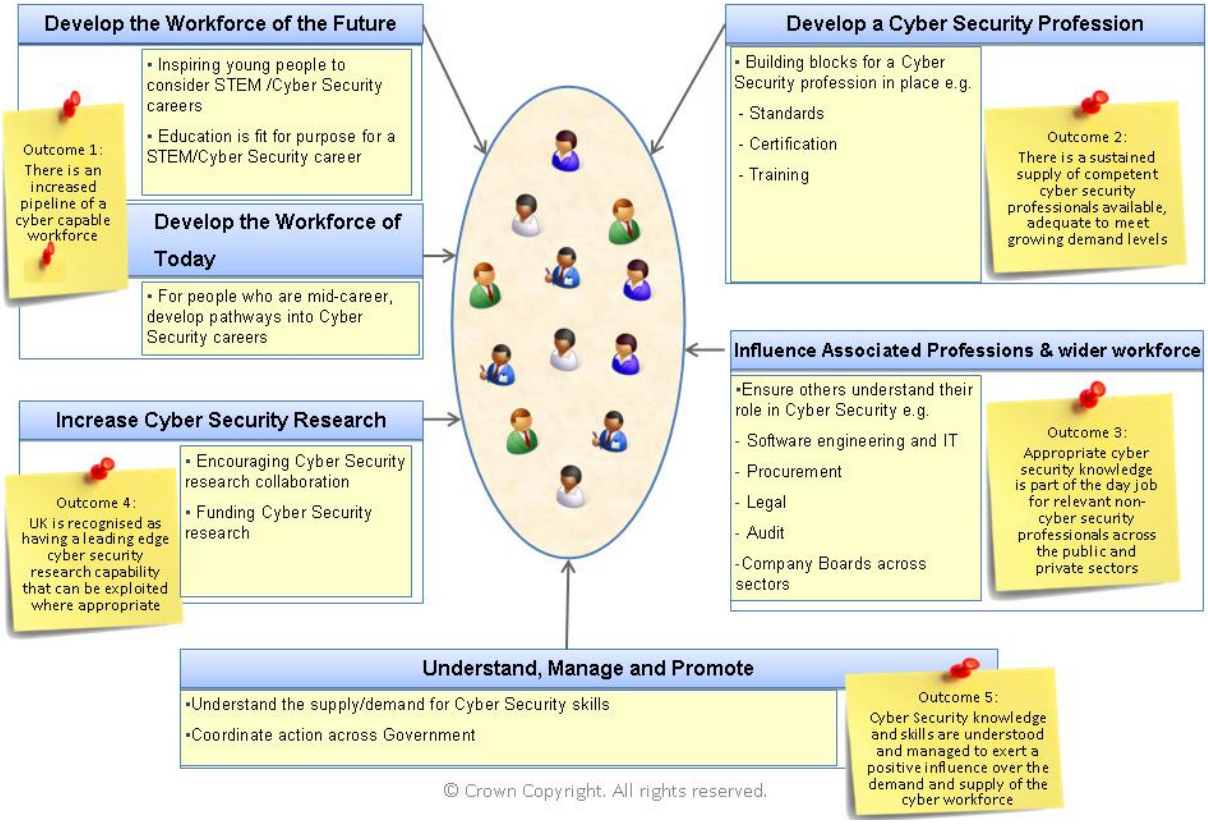


Source:[4]

1.3 Through the National Cyber Security Programme (NCSP) the Department for Business Innovation and Skills, GCHQ and the Cabinet Office have partnered to lead and support activity to increase cyber security skills at all levels of education, and amongst the cyber security workforce (both public and private sector). This work has been taken forward in close collaboration with business and the education and skills sectors. NCSP activity to deliver Objective 4 is based around 5 key building blocks, set out in the diagram below.

[2] Frost and Sullivan Consultants (2013) *The 2013 (ISC)2 Global Information Security Workforce Study*
[3] Department for Business Innovation and Skills (2013) *2013 Information Security Breaches Survey: Technical Report*
[4] Department for Business Innovation and Skills (2013) *Competitive analysis of the UK cyber security sector*

NCSP activity to deliver Objective 4 of the National Cyber Security Strategy



1.4 The progress that has already been made – ranging from innovative activities to promote cyber security learning in schools to the accreditation of information security professionals under CESG's Certified Professional scheme – is set out in *Progress Against the Objectives of the National Cyber Security Strategy* December 2013. Our efforts to increase cyber security skills are also closely aligned to, and benefit from a a range of wider Government initiatives. This includes action to strengthen digital skills across the information economy, promotion of STEM (Science, Technology, Engineering and Maths) subjects and careers, apprenticeship reforms and work to strengthen links between business and universities.

1.5 We need to build on this strong foundation to enable transformational change, ensuring that a focus on cyber security skills is firmly embedded across all sectors. At the same time we need to be sure that all the activities we are involved continue take account of the changing cyber security landscape, and the evolving needs of businesses. To this end, we have engaged with a range of businesses to discuss their cyber security skills needs through a questionnaire and series of workshops (details of our methodology are at annex A). The exercise included businesses that employ cyber security professionals because they face a significant cyber threat and businesses that supply cyber security products and services. Key findings are set out in chapter 2 whilst chapter 3 summarises our plans for cyber security skills activities in the coming year, informed by the suggestions of businesses who participated in the exercise.

1.6 There will of course be other perspectives on the challenges faced by industry and how they can be best addressed, including from those involved in the provision of education and skills training. We will continue to work closely with these organisations, supporting them to showcase the work they are doing to increase the supply of excellent cyber security skills, to strengthen links with businesses and to share ideas for the future.

Chapter 2: Key Findings

2.1 This chapter summarises the key points made in the questionnaire and workshops in relation to:

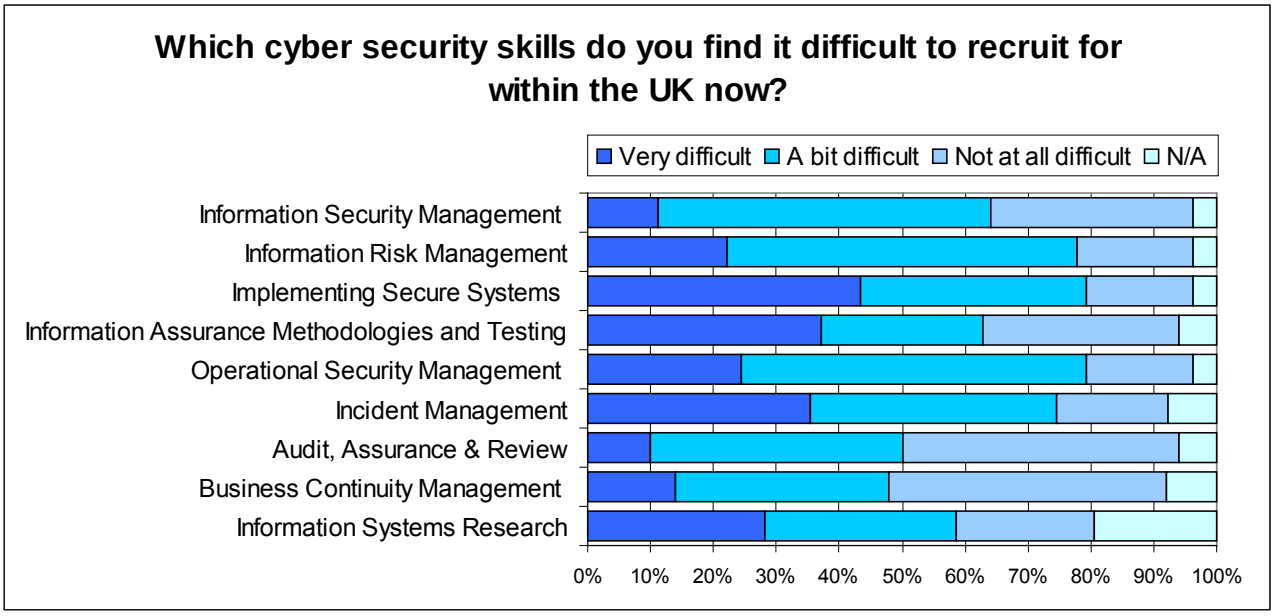
- cyber security skills shortages
- sources of cyber security skills
- business-led skills development activities; and
- business engagement with national skills interventions.

Full questionnaire and workshop outputs can be found in the supporting evidence accompanying this report.

Cyber skills shortages

Nature of skills shortages

2.2 Recruitment of individuals with technical cyber security skills[5] was considered difficult by the majority of participants. In the questionnaire, the greatest difficulty was reported in recruiting individuals with skills in implementing secure systems, followed by operational security management, incident management and information risk management.



2.3 An area of consensus amongst workshop participants was the shortage of well developed soft and business skills, particularly amongst recent graduates. These were seen as essential for explaining threat and solutions to company boards or customers, balancing business and security priorities effectively and delivering cultural change.

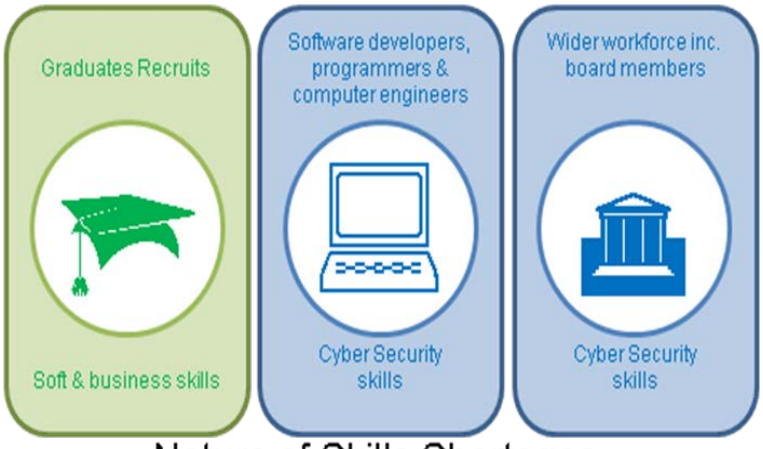
[5] As set out in the IISP skills framework

2.4 The workshops also raised concerns about a shortage of skills required to support development of security in emerging technologies and practices, e.g. increased business use of mobile devices, social media and 'bring your own device'.

2.5 It was noted that there is a particular shortage of women coming into the profession (only one in 10 cyber security professionals are women[6]). This needs to be addressed in order to increase the scale and diversity of the cyber security talent pool.

2.6 There was also widespread agreement on the shortage of cyber security skills amongst software developers, programmers and computer engineers. Embedding greater awareness of cyber security amongst these professions and education pathways towards them was seen as important in increasing the inherent security of information and control systems, and reducing the long-term demand for remedial work by cyber security professionals. It was acknowledged that to be effective this needs to be accompanied by increased demand for software that is robust and secure.

2.7 Finally, participants raised concerns about the lack of cyber security skills in the wider workforce. In particular, it was felt that a lack of cyber security skills amongst Board members (outside the supplier sector) had consequences for their understanding of the threat facing their business, and for their willingness to invest in the skills required within their organisation to respond effectively.

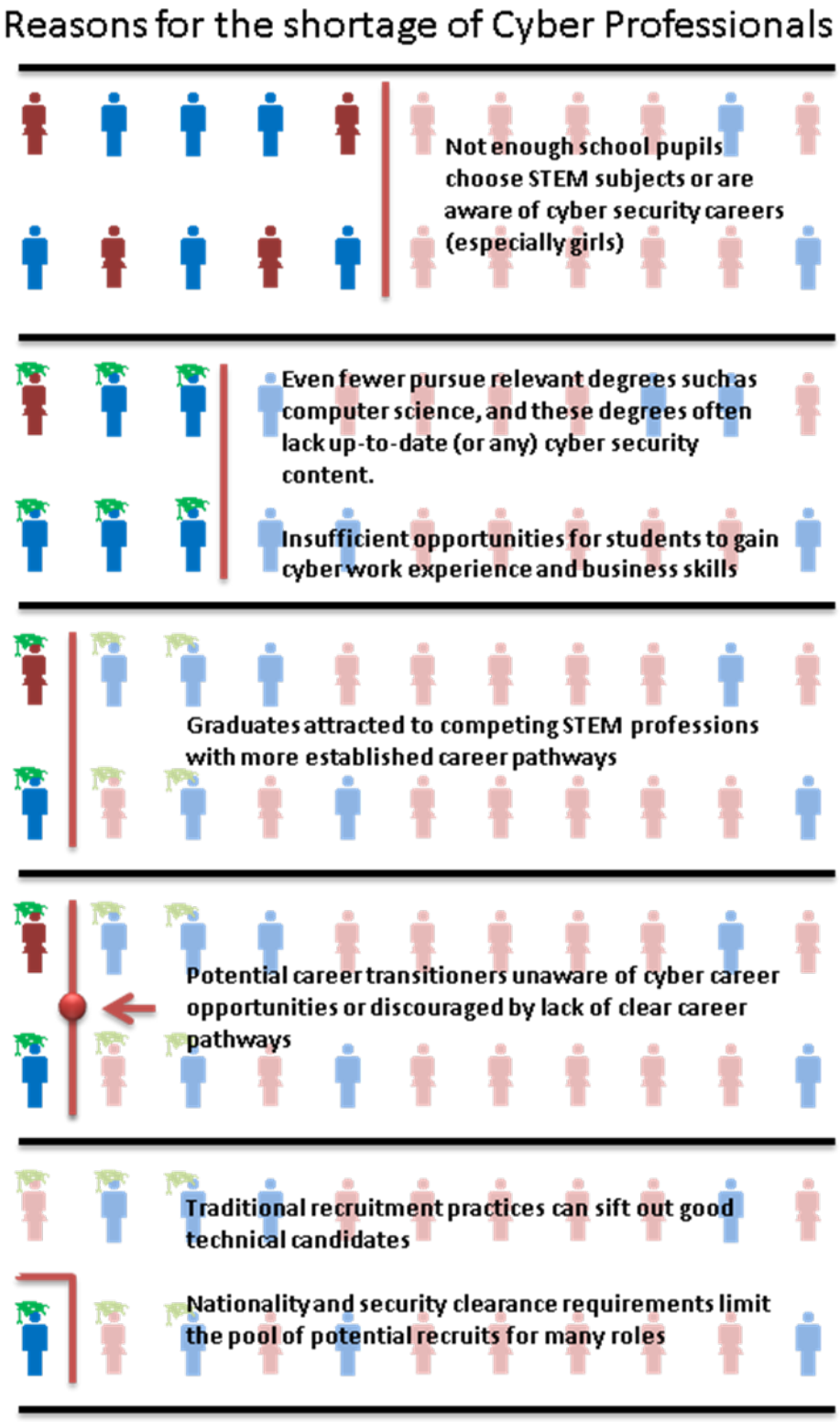


Nature of Skills Shortages

[6] Career Analysis into Cyber Security:New and evolving occupations -E-Skills UK & Alderbridge 2013

Reasons for cyber skills shortage

2.8 Participants identified a range of reasons for skills shortages (set out in the infographic below) from low take-up of STEM subjects in schools, through to business recruitment practices. Government has a role in addressing a number of these issues, described further in chapter 3.



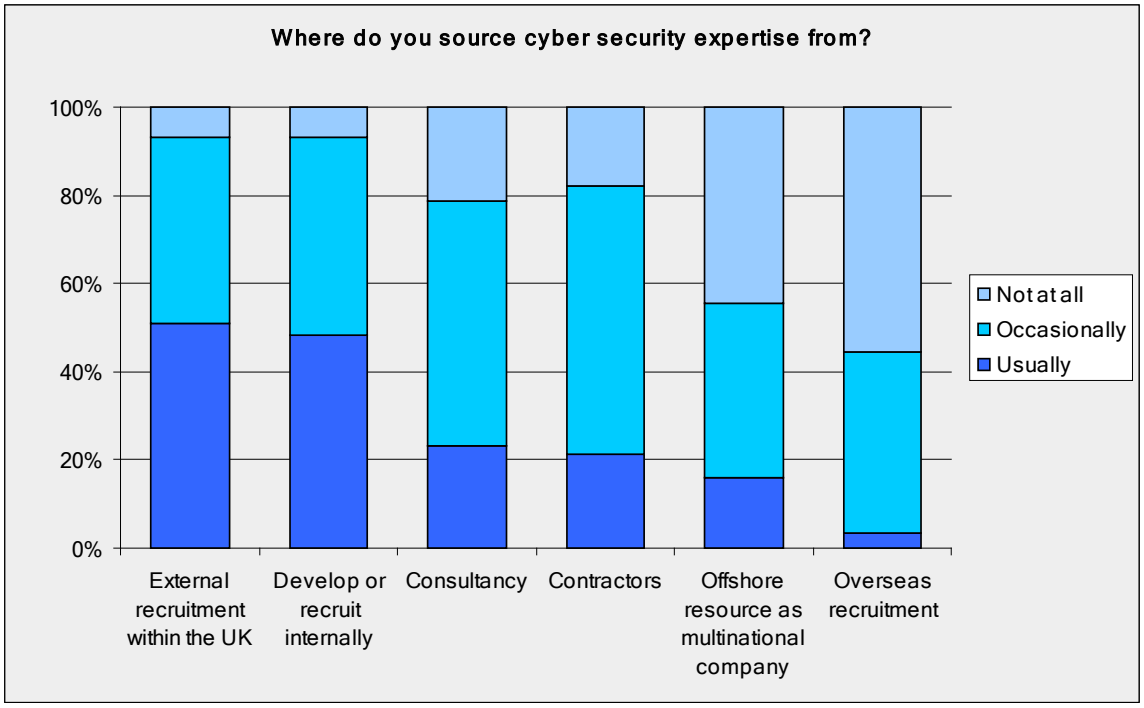
Consequences of skills shortages

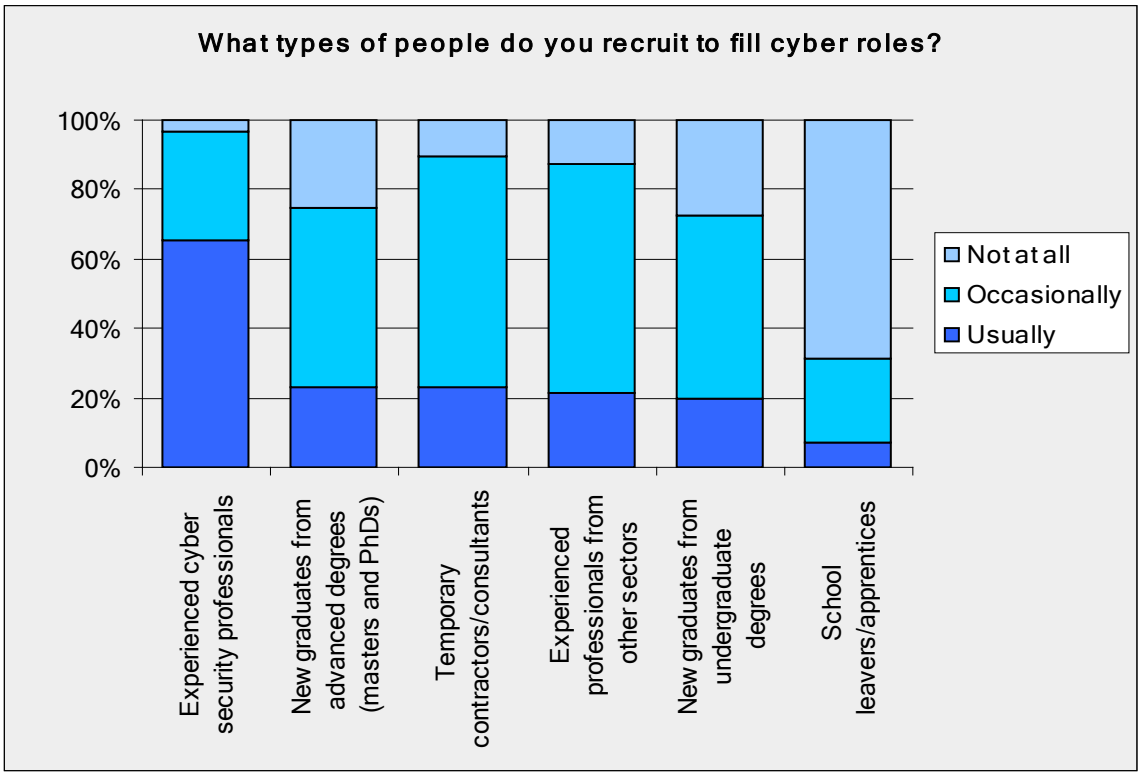
2.9 Immediate consequences of these shortages reported included inflated salaries, retention problems (particularly for SMEs) and an ageing and largely male workforce. Cyber suppliers reported an impact on their ability to grow their business. Other businesses were concerned about the impact on the cost and effectiveness of their efforts to protect their organisation.

Sources of cyber security skills

Recruitment practices and people

2.10 Both questionnaire and workshop participants tended to recruit from within the UK rather than overseas, primarily through external recruitment and developing and recruiting staff internally. The charts that follow show questionnaire respondents' main sources of cyber security expertise:





2.11 Workshop participants suggested that recruitment was often via informal routes and headhunting rather than open competition. It was noted that given the relative immaturity of the cyber security profession, many existing professionals have ended up there by accident rather than design. A general theme was that experience was valued more highly than qualifications. In turn, professional qualifications were valued more highly than academic qualifications. However, there were some differences between cyber suppliers and other organisations.

2.12 The cyber supplier sector was more focused than Critical National Infrastructure (CNI) organisations on recruiting and developing new talent, largely graduate plus a few examples of school leavers. This was partly due to necessity (for example, SMEs reported difficulties competing with larger companies for experienced professionals) but young recruits were also said to be valued for innovation and lateral thinking skills. By contrast, CNI and retail sector participants in particular focused recruitment on experienced professionals and consultants, and some contracted out the majority of their cyber security provision. It was noted that a reliance on experienced professionals was not sustainable without a willingness from businesses to provide individuals with the opportunity to develop that experience. A reliance on contractors could leave an organisation without the long-term capacity and experience to make informed business decisions about cyber security risk and mitigations.

2.13 Participants suggested that career transitioners represented an important source of mature yet fresh cyber security talent for many businesses, notably from the Armed Forces, Security Services, Police and IT sectors. It was noted that this has implications for retention within these organisations, although there were good opportunities for mutual benefit where headcount was being reduced, notably from the Armed Forces.

Qualifications

2.14 Only a few organisations reported preferentially recruiting graduates from specialist cyber security undergraduate degrees. More commonly graduate recruits had completed STEM degrees (often computing-related), or sometimes courses in other disciplines. Businesses did not generally value masters degrees more highly than undergraduate degrees, although there were some exceptions to this. Whatever the degree course, businesses indicated that most graduates require significant training once they join the organisation.

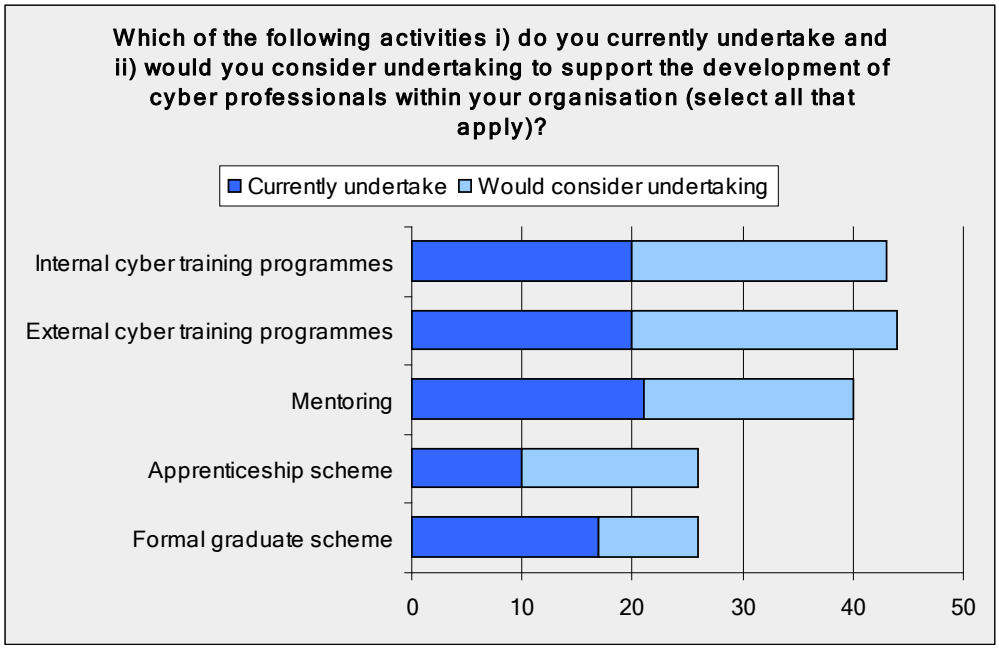
2.15 Businesses looked for a wide range of professional qualifications and accreditations, with questionnaire respondents most commonly citing CISSP, CISM, ISO27001LA, CLAS and CISA. Some workshop participants also mentioned that they look for IISP membership and accreditation amongst their cyber security workforce.

2.16 In general it was felt that professional qualifications were more useful than advanced-level academic study, particularly in demonstrating competence to customers. However, some mentioned that the array of qualifications and accreditations can be confusing and there may be more than is necessary. It can be resource intensive for individuals/companies to maintain the range of accreditations/professional body memberships deemed necessary to secure business.

Business-led skills development activity

Workforce of today

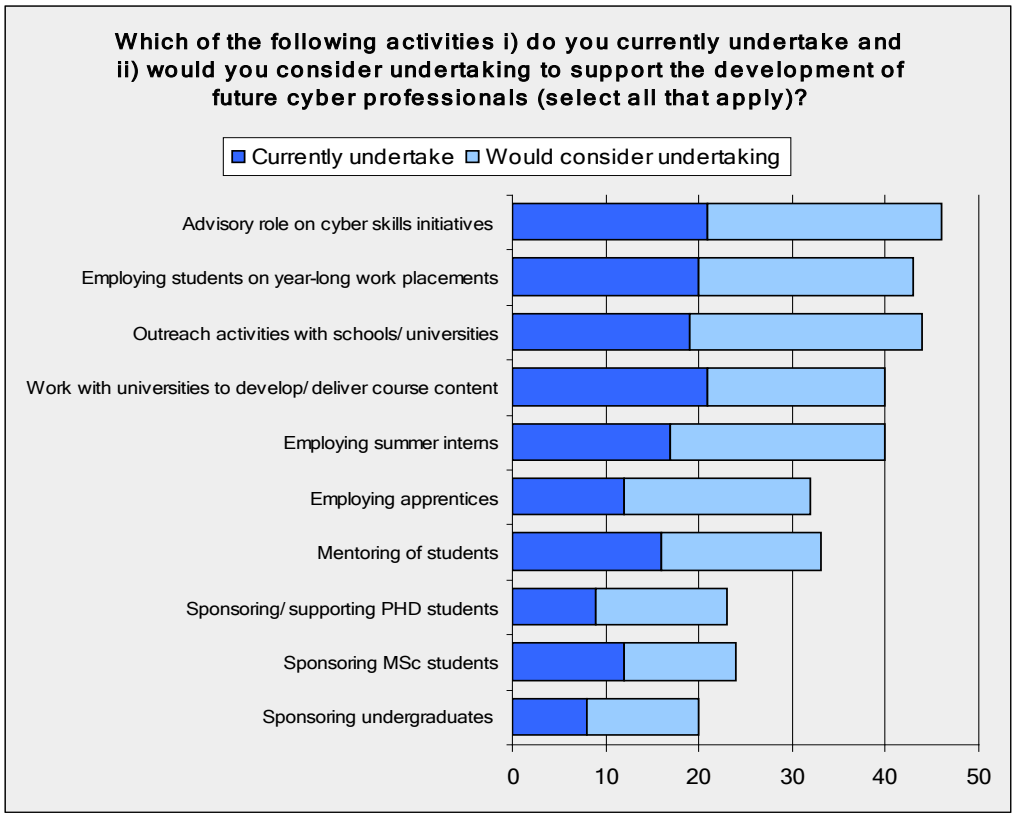
2.17 Around 60% of questionnaire respondents reported some activity to support the development of cyber professionals within their organisation. The graph below shows how many of the businesses surveyed provide different opportunities, or would consider doing so.



2.18 Feedback from the workshops suggested that large cyber suppliers tend to have the most extensive training programmes for new staff, sometimes involving months of intensive training. SME cyber suppliers reported a more personalised approach to learning and development, focused on coaching and one to one support. Given the focus of CNI companies on recruiting experienced cyber professionals, there was an expectation that new staff should already have the skills they need to hit the ground running. CPD tended to be based on individual needs, and was sometimes linked to securing or maintaining a range of professional qualifications and accreditations.

Workforce of the future

2.19 Around 60% of questionnaire respondents reported some activity within their organisation to support the development of future cyber professionals, with cyber suppliers more likely than other respondents to do so. This difference was reflected in feedback from the workshops. The graph below shows how many of the businesses surveyed are involved in different activities, or would consider involvement.



2.20 A range of businesses participating in the workshops were involved in work with schools, the Cyber Security Challenge and efforts to increase diversity in the cyber security profession. Some businesses were working with a university on the design or delivery of course content and others were keen to do so in the future, acknowledging that this was important in helping to ensure that graduates meet employer needs. However, this was often based on personal relationships with particular academics and it could be difficult to know how to get involved with universities. Some companies had employed interns or students on sandwich placements and saw value in doing so. Whilst others thought it would be difficult to employ an intern for a variety of reasons, there was general recognition that businesses need to provide more opportunities for students to gain work experience. A few companies reported work with Centres of Doctoral Training and had sponsored PhDs.

2.21 A few companies represented at the workshops were already employing apprentices and there was significant interest from others in doing so in the future. It was seen as a good way of growing and embedding talent in an organisation. The new e-skills UK Cyber Security Apprenticeships (both at Advanced and Higher level) scheme was widely welcomed because it had been designed by employers, and would make it easier for businesses to take on and train apprentices. It was acknowledged that time and effort was required to train apprentices, and that they were not appropriate for all roles.

Business engagement with recent national cyber security skills interventions

2.22 We were keen to understand more about employer engagement with some of the national activities that Government has funded over the last year (e.g. pilots on cyber internships for higher education students and employer bursaries for cyber MSc students[7]) where translating initial business interest into definite commitments of support has been challenging.

2.23 Discussion in the workshops and questionnaire responses indicated that a lack of awareness (particularly amongst company decision makers) about the schemes was likely to be one of the main reasons for limited take-up. Those who were aware of the schemes felt that the benefits to business (as opposed to students) of participation needed to be clearer. Selling the benefits was considered to be particularly challenging given the immaturity of the cyber profession (compared to, for example, engineering) and low Board-level engagement. Some cited a lack of time and resources to engage in the schemes. For internships in particular, it was felt that flexibility over the length of placements, and longer lead-in times that take account of business planning cycles would help to increase employer engagement. Problems of security clearance were also perceived to be a barrier to employing interns for some firms. It was felt that there was insufficient broad demand for employees with cyber security MSc degrees to make a national sponsorship scheme viable.

2.24 Awareness of new Government-backed schemes to establish cyber security Centres for Doctoral Training and cyber security apprenticeships was also relatively low, emphasising the need for promotion of these schemes amongst employers.

[7] The internship pilot for higher education students interested in working in cyber security was run by the Information Assurance Advisory Council. The Cyber Security Masters bursary pilot scheme was run by the Institution of Engineering and Technology on behalf of the Cyber Security Skills Alliance. BIS provided financial support for both pilots with NCSP funding.

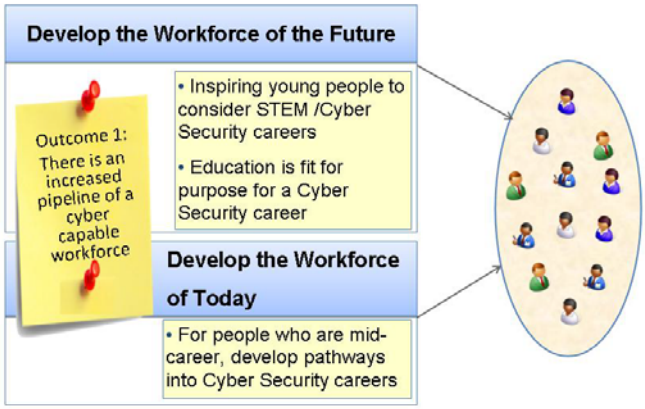
Chapter 3: National Cyber Security Programme Skills Plan for 2014-15, informed by business suggestions

3.1 This chapter sets out our plans for cyber security skills activities in 2014-15, informed by suggestions from participants in this exercise for what more needs to be done to boost the capability of the cyber workforce today and the pipeline of future cyber talent.

3.2 Our programme of work in 2014-15 will build on the wide range of cyber security skills activity undertaken since the inception of the NCSP, based on the core elements described on page 9. We have included other publicly-funded activities beyond the NCSP where these support delivery of the National Cyber Security Strategy, notably activities delivered by e-skills UK and funded via the UK Commission on Employment and Skills (UKCES), and DfE support for teaching of the new school computing curriculum.

3.3 The full set of suggestions made by businesses, along with the Government response to each of them, can be found in chapter 3 of the supporting evidence accompanying this report.

Develop the workforce of the future and the workforce of today



Education in schools

Business suggestions

3.4 Business feedback underlined the importance of embedding cyber security into school-level education, both within the new computing curriculum and wider school activities, to raise awareness about cyber security careers, encourage take-up of relevant STEM subjects and educate students to be effective members of the broader digital economy. This is particularly important for girls, who are currently far less likely than boys to pursue a cyber career. Participants felt that initiatives in this space should be a collaboration between Government, skills delivery partners and industry, which has an important role to play in building real-world credibility into cyber security education.

Working with business and delivery partners, in 2014-15 we will:

Fund British Computing Society (BCS) to provide **support for teachers to implement all elements of the new computing curriculum**, including the aspects relevant to e-safety. This includes £25k tax free **scholarships for Computer Science trainee teachers** who have the potential to become future school leaders (selected by top tech employers) and the **recruitment of 400 Computer Science Master Teachers**, who will provide CPD to 16,000 teachers a year, supported by top employers.
Fund e-skills UK and teachers' network, 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.
Fund e-skills UK to develop cyber security **teaching and learning materials for key stage 3 pupils This will build on** successful projects that develop equivalent materials for GCSE and A-level, and target learners early enough to influence their GCSE options. Linked to this, e-skills UK will roll-out their Secure Futures schools campaign in London, Greater Manchester and Sussex with the support of employers, following a successful pilot in Worcestershire.
Continue to fund the **Cyber Security Challenge schools programme,** complementing the e-skills UK activity above.
Support the award winning ***Computer Club For Girls*** programme delivering "coding" courseware sponsored by industry to 11-14 year old girls.
Continue to fund STEMNET to run the **STEM Ambassadors** programme, a nationwide network of over 27,000 volunteers (40% female) from science, engineering and technical companies or academia, who work with UK schools to raise awareness of STEM careers and provide stimulating activities to increase their interest in STEM subjects. We are keen to increase the number of STEM ambassadors directly drawn from the cyber profession (currently around 100).

Higher Education

Business Suggestions

3.5 Business feedback emphasised the importance of developing closer working relationships between academia and industry 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) better meet industry needs. There was thought to be an opportunity for greater innovation in higher education, for example, linking professional and academic qualifications more closely. It was suggested that work experience should be a core part of degree qualifications to increase students' real-world experience, and that businesses should provide work experience opportunities for students through internships, work placements, projects

etc. Businesses would welcome any support available to overcome security clearance issues.

3.6 Businesses suggested that given limited industry demand, the 2013 Cyber Security Masters Bursary pilot should not be rolled-out more widely.

Working with business and delivery partners, in 2014-15 we will:

Fund the Higher Education Academy to i) provide universities with **grants for innovative proposals to improve cyber security teaching** (e.g. university/employer partnerships, innovative course delivery methods such as Massive Open Online Courses (MOOCs), incorporating professional qualifications into degrees); and ii) promote excellence in cyber security teaching across the Computing Network e.g. through events and sharing best practice.
Accredit **Academic Centres of Excellence for Cyber Security Education**, complementing the existing Academic Centres of Excellence in Cyber Security Research (ACE CSRs). Criteria are being developed in consultation with industry and academia. As an initial step, GCHQ intends to identify high quality cyber security MSc courses through a new certification scheme.
Fund e-skills UK, via UKCES, to deliver a UK **Cyber Security HE internship scheme**, facilitating the provision of industry internship placements of varying lengths for students during or after their degrees. This builds on the 2013 IAAC Cyber Internships Pilot and previous best practice by e-skills UK, The Council of Registered Ethical Security Testers (CREST) and others.
Continue to fund the **Trustworthy Software Initiative** to develop learning materials on developing safe and secure software that universities can use free of charge to deliver learning outcomes on information security for students studying a range of computing degrees, beginning with software engineering. In the longer term this will be supported by amendments to **accreditation requirements for all degrees accredited by the IET and BCS to include mandatory learning outcomes on information security**.
Include cyber security in wider planned initiatives aimed at **strengthening teaching in Computer Science degrees**, including a) a **forum or network** to foster relationships between industry and academia, b) a programme to identify different ways for **lecturers to spend time in industry** - e.g. placements, projects and c) supplementary modules for degree level students, potentially delivered through a MOOC, to improve their **business skills**.

Apprenticeships and vocational education

Business Suggestions

3.7 There was wide ranging support from businesses for the idea of apprenticeships as an alternative route into the cyber security profession, and in particular for the e-skills UK new Cyber Security Higher Apprenticeship scheme. Participants at the workshops stressed the importance of the training provision meeting industry needs and of

promoting the benefits of apprenticeships with both employers, and school pupils, parents and teachers.

3.8 To date, efforts to increase teaching about cyber security have focused on schools and higher education. The demand for new vocational qualifications to support the cyber security apprenticeship framework has highlighted a need to explore what opportunities currently exist within the further education (FE) sector, and what more might be done to support vocational routes into the cyber security profession.

Working with business and delivery partners, in 2014-15 we will:

Fund e-skills UK, via UKCES, to deliver the new employer-led **cyber security Apprenticeship (Advanced and Higher) scheme**, designed by employers to ensure it meets business needs. The Higher Apprenticeship will include on the job experience, vocational training and a foundation degree. The benefits for employers of taking on apprentices are set out in the *Guide for Industry.* **Marketing of the scheme to young people, teachers and parents** will be an important element of the programme, complemented by high profile national campaigns by the National Apprenticeships Service to promote apprenticeships more generally.
Continue the **SIA Higher Apprenticeship Scheme** to attract motivated and technically-minded people to join the Intelligence Academy. The apprentices will undertake a structured training programme that will equip them with the cyber skills and experience necessary to enable them to build, develop and further advance the Agencies technical capability in the future.
Working with providers of vocational qualifications and wider FE stakeholders, explore opportunities to **strengthen cyber security education at FE level**, e.g. potentially encouraging the development of further dedicated cyber qualifications or the inclusion of cyber security components in appropriate computing and STEM courses.

Developing pathways into the profession

Business Suggestions

3.9 There was strong feedback that Government, businesses and skills bodies need to work together to increase awareness of the cyber security sector as a 'profession' with an attractive career path. Clear learning and career pathways should be created and promoted to university students and professionals from related disciplines. There was support for the use of competitions, gamification and media coverage to promote the exciting opportunities presented by a cyber career.

3.10 There was also support for the idea of career transition programmes, to bring people (particularly from the military) into the cyber security profession. It was also suggested that there should be national recruitment events to help publicise job opportunities, particularly in SMEs.

Working with business and delivery partners, in 2014-15 we will:

Continue to support e-Skills UK, working with IISP and employers, to develop (as required) and promote the uptake of **learning pathways** which are linked to national skills standards and aligned to selected roles within the CESG Certified Professional (CCP) scheme.
Work with CREST to promote **on-line resources illuminating routes towards a wide range of cyber security roles** produced with funding from BIS.
Continue to sponsor the **Cyber Security Challenge and the National Cipher Challenge**, which use gamification as well as careers fairs to attract students and existing professionals into cyber security, creating opportunities for employers and talent to come together. In 2013 the Challenge attracted over 2000 new joiners.
Include cyber security in a **national campaign to communicate the range of exciting digital careers**, and in **career profiles and supporting career material** to help academia showcase the range of careers open to those that study Computer Science.
Support and promote the activities of the **Women's Security Society**, which aims to advance women working in, or moving to, today's security industry.
Continue to support the **CompTIA 'Armed for IT' initiative** which is focused on supporting service leavers into information technology and cyber security careers.

Develop a Cyber Profession

Business Suggestions

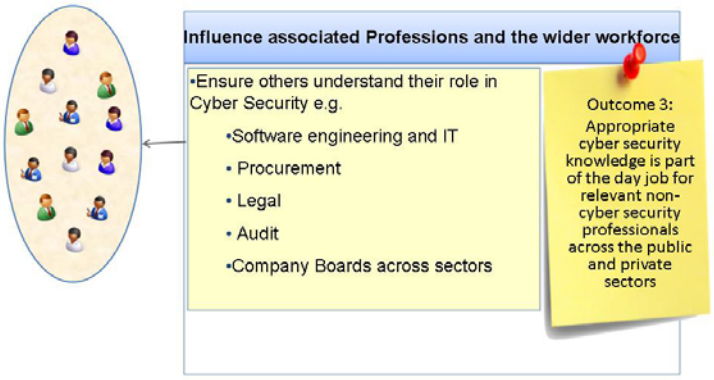
3.11 Businesses stressed the importance of creating a cyber security 'profession'. This was thought to be critical for the long term growth and sustainability of the UK's cyber security capability. IISP was established in 2006 as an independent accreditation authority advancing the professionalism of information security practitioners and provides a widely accepted skills framework for the profession. A wide range of additional professional qualifications and accreditations have been established in recent years in response to demand from industry and Government for evidence of professional competence in different aspects of cyber security. It was suggested that rationalisation of these qualifications, or guidance to help employers and professionals identify the most high quality/ relevant of these would be useful.

3.12 It was recognised that the CCP scheme, which uses the IISP skills framework as its basis, has helped to provide clarity and assurance in relation to the skills and competence required by those working on Government projects. It was suggested that the scheme could become a nationally recognised scheme for industry and local government. Finally, it was suggested by some that there should be one specific qualification which qualifies you to be a cyber security professional, along the lines of the 'chartered status' used in professions such as engineering.

Working with business and delivery partners, in 2014-15 we will:

Continue to expand the **CCP Scheme** by promoting the scheme in the private sector and adding additional roles (including those suggested by businesses) that have the widest applicability (e.g. penetration tester). Professionals will continue to be certified by three certifying bodies, the BCS, APM Group and a consortium of IISP, CREST and RHUL.
Develop (through GCHQ) a process to **accredit private sector training** which supports cyber security professionals to gain the skills needed for specific roles within the CCP Scheme. The scheme will provide a level of confidence that the cyber security subject material and the teaching are at an approved level. Relevant courses accredited under this scheme will be eligible to be showcased on e-skills UK's Cyber Academy Learning Pathways.
Work with e-skills UK, IISP and employers to promote the application of **National skills standards in Cyber Security** (developed by e-skills UK and IISP)**,** which are mapped against the IISP skills framework and aligned to selected roles within the CESG Certified Professional (CCP) scheme.
Support e-skills UK and its partners to roll out the **CPD centre** in Malvern aimed at local SMEs to increase their organisational cyber security skills.
Explore with professional bodies, businesses and others whether there is a demand for a **'chartered status'** for cyber professionals.

Influence Associated Professions and the wider workforce



Business Suggestions

3.13 Businesses suggested that steps should be taken to improve company boards' skills in understanding and managing cyber risks e.g. through including cyber security in MBAs and training for Company Secretaries and Directors. This would underline the importance of investment in a company's cyber security capability, building on the positive start made by the '10 Steps' guide and Cyber Governance Health Check.

3.14 It was also suggested that all staff, particularly in high threat organisations should have a basic understanding of cyber security and the need to protect information. We need cultural change so that cyber security is not seen just as an IT problem. It was suggested that cyber security training appropriate for the wider workforce could be delivered through a MOOC.

3.15 It was widely suggested that cyber security should form a key part of the training and ongoing professional development for software engineers and IT professionals.

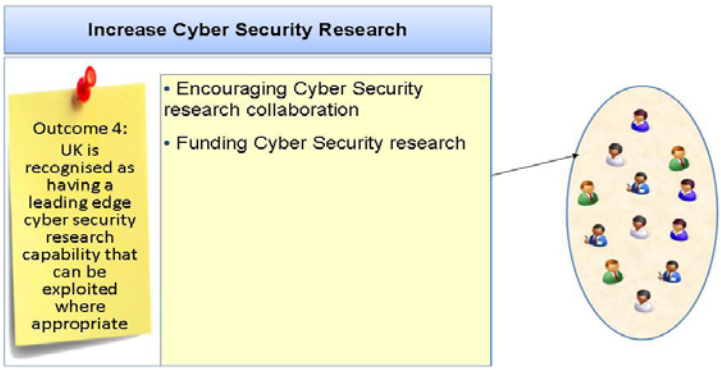
3.16 Finally, it was suggested that more should be done to educate procurement departments in Government and the private sector about how cyber security should be factored into IT and other relevant contracts, and the professional or academic qualifications that those providing cyber security services should have.

Working with business and delivery partners, in 2014-15 we will:

Repeat the **Cyber Governance Health Check Tracker** in 2014 to benchmark against the 2013 results, and indicate what measures boards can undertake to show leadership in risk mitigation. We will also seek to use the Tracker commissioning as a route for promoting the guide for industry on cyber skills interventions.
Develop specific **guidance for the investor community**, providing them with key questions to ask boards, including references to skills and training.
Develop specific **guidance for Non-Executive Directors** (NEDs) 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. We will also continue to provide **cyber security and information assurance training to NEDs and Board Members throughout the public sector**.
Continue to stress the need for a more informed and risk aware workforce through **marketing of the 10 Steps guidance and other key sectoral and corporate governance interventions**.
Continue to require public sector staff to undertake a '**Responsible for Information' e-learning course** and look to adapt the course for the use of private sector organisations, in particular SMEs who may not have their own in-house training.
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 businesses.

We will work with our academic and industry stakeholders to encourage uptake of the course.
Support the IET and BCS in developing a requirement for **engineers and IT professionals registering with them to demonstrate awareness of information security**, building on the forthcoming requirement for all computing-related degrees accredited by the IET and BCS to include information security learning outcomes.
Work 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.
Encourage **Law Society and ICAEW (Institute of Chartered Accountants of England and Wales) members** to undertake basic cyber e-training to improve their understanding of their responsibilities to protect confidential information and to increase their confidence when talking to their clients about cyber risk.

Increase Cyber Security Research

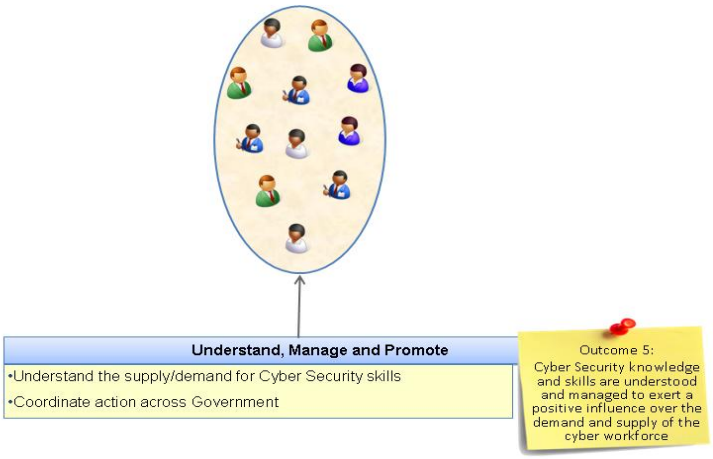


3.17 Whilst the business engagement exercise did not explicitly seek suggestions in relation to cyber security research, building a cutting edge research capability forms part of our strategy for increasing high-end cyber security skills capability, as well as ensuring a strong UK knowledge base. For completeness, we therefore set out our plans to increase cyber security research below.

Working with business and delivery partners, in 2014-15 we will:

Continue to work closely with the 11 **Academic Centres of Excellence for Cyber Security Research** (ACE-CSRs), invite applications from other universities wishing to gain ACE-CSR accreditation, and encourage business investment.
In partnership with Research Councils UK (RCUK), continue to fund two **Centres of Doctoral Training (CDTs)** to deliver multidisciplinary training and provide the skills needed by the next generation of doctoral-level cyber security experts. The CDTs are engaging with businesses to ensure the training reflects the complex and dynamic nature of cyber threats. These centres will deliver 66 additional PhDs by 2017. In parallel GCHQ will continue to take forward their PhD studentship programme with NCSP funds.
In partnership with RCUK, continue to fund and support three **Cyber Security Research Institutes**, which facilitate collaboration between different universities and academic disciplines on important cyber research problems.

Manage, understand and promote



Business Suggestions

3.18 Business feedback stressed the importance of strong leadership within Government to deliver change in this area, and presenting Government interventions as part of a coherent strategy to boost cyber security skills, rather than stand-alone initiatives. It was suggested that cyber security skills activity should feature in related strategies, such as the Information Economy Strategy and London Business Crime Strategy. Participants raised the importance of increasing industry awareness of cyber security skills initiatives and promoting the benefits of participation to increase industry leadership and investment in this area. Participants also stressed the need for early and ongoing engagement with business on design, delivery and evaluation of interventions.

Working with business and delivery partners, in 2014-15 we will:

Continue to show **leadership on the cyber skills agenda**, collaborating across Government and with our partners to fund and promote interventions at every level of the education and skills system to deliver objective 4 of the National Cyber Security Strategy.
Develop and promote ***Cyber Security Skills: A Guide for Business*** to showcase the opportunities and benefits for businesses of involvement in skills and research activities.
Continue to work closely with businesses and academia at a strategic level to understand demand and supply, and strengthen skills activity, e.g. through the skills, education and innovation workstream of the Cyber Growth Partnership.
Recognising that cyber security does not exist in a vacuum, work across Government and with partners to ensure that the importance of **cyber security skills and capability is reflected in relevant strategies and plans**, for example, those related to the wider Information Economy or business crime.

Conclusion

4.1 This exercise has helped us to understand the different perspectives of businesses on the cyber security skills challenges they face, and their ideas for how they can be best addressed. These ideas have helped to inform our future plans for increasing the UK's cyber security skills and capability, whilst reaffirming that existing activity to deliver objective 4 of the National Cyber Security Strategy is appropriately targeted.

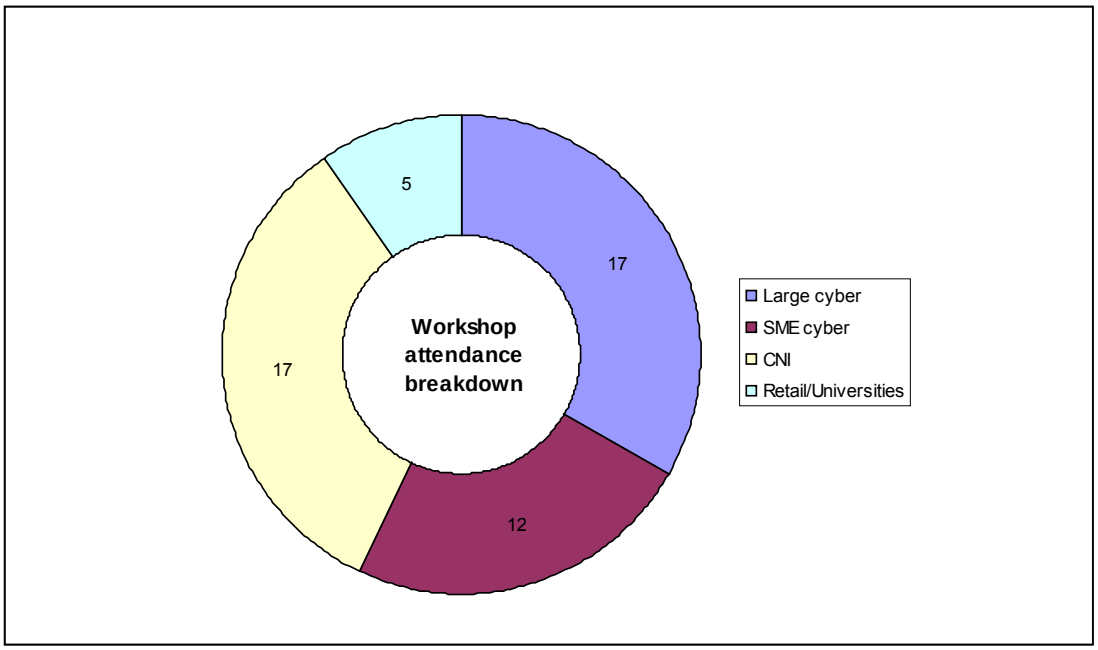
4.2 It is important not to underestimate the scale of the challenge that faces both businesses and Government in securing the skills required to meet increasing demand. We need to create a cyber security profession which attracts talented individuals who go on to receive the education, experience and professional support they need to become experts. We need to strengthen cyber security skills in associated professions such as IT, software design and procurement to ensure that cyber security is 'built in' to software, infrastructure and services. And we need to educate the wider workforce, particularly at Board-level, to ensure that businesses, as well as public sector organisations, have the capability to understand and respond effectively to cyber security risks.

4.3 Working in partnership across Government, business and the education and skills sectors we have already made significant progress. Strong business leadership is becoming increasingly important as we seek to embed cyber security skills more deeply in the fabric of organisations, and strengthen the pipeline of future talent. Many businesses are already showing this leadership, and others are keen to do so, recognising the opportunities and benefits for their organisation. Our new *Cyber Security Skills: Guide for Business* will help them to identify excellent practical opportunities to support the development of cyber security skills.

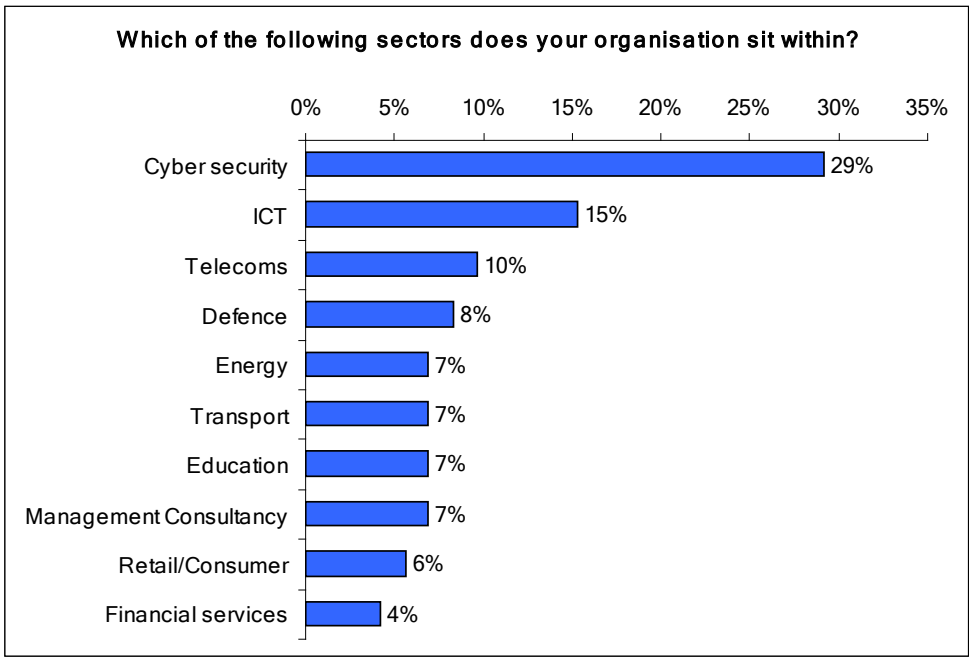
Annex A: Methodology

2.1 The business engagement exercise consisted of a series of workshops and an online questionnaire. We talked to businesses in the cyber supplier sector and businesses that employ cyber security professionals because they face a significant cyber threat.

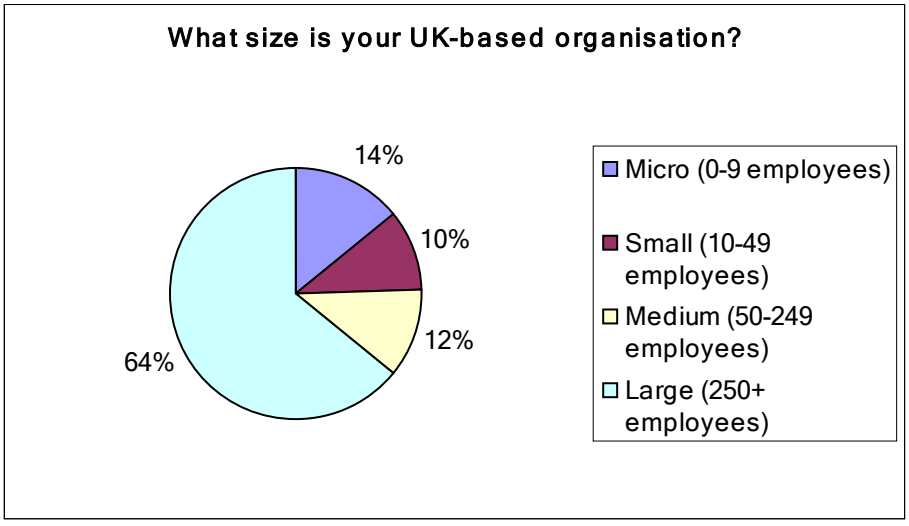
2.2 Four workshops were run in December 2013, with 51 participants from businesses representing large cyber suppliers (including some IT and defence companies), SME cyber suppliers, Critical National Infrastructure companies (energy, finance, transport, telecoms), and retail companies and universities. Participants were invited to the workshops on the basis of their known interest in cyber security. The workshops were supported by colleagues from e-skills UK, Tech UK, the Institution of Engineering and Technology (IET) and the Malvern Cyber Security Cluster.



2.3 The questionnaire ran for a month in late 2013. It was promoted through a wide range of partners in Government, skills organisations and trade associations. 81 responses to the questionnaire were received. Questionnaire respondents came from the following sectors:



2.4 The majority of questionnaire respondents were from large businesses:



Issues covered in the questionnaire and workshops

2.5 The workshops and questionnaire covered the following issues:

a. what businesses see as their main cyber skills shortages and skills sources;
b. what businesses currently do, or would consider doing, to support the development of their own cyber professionals, and the cyber workforce of the future;
c. business engagement with national skills interventions; and
d. recommendations for what more should be done to boost the capability of the cyber workforce today and the pipeline of future cyber talent.

2.6 Whilst our primary focus was on skills for cyber security specialists, discussions also extended to the importance of cyber skills amongst associated professions and the wider workforce, and in particular, board-level decision makers.

Limitations

2.7 This exercise 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. This was appropriate to meet our needs but has a number of limitations. The participants were drawn from a wide range of companies, but they were inevitably self-selecting. It is likely that those who were willing to take the time to participate already have some appreciation of the importance of cyber security skills. The benefit of this was a well-informed debate, the disadvantage was that the views of less-informed businesses will not be reflected in our findings. Whilst the workshop format was a useful way of generating and discussing ideas, it can be difficult to assess how widely a view is held. The survey ensured that everyone had the opportunity to participate, but the relatively small sample makes meaningful quantitative analysis difficult.

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/14/647