HM Government

INITIAL NATIONAL CYBER SECURITY SKILLS STRATEGY

INCREASING THE UK'S CYBER SECURITY CAPABILITY

A CALL FOR VIEWS

EXECUTIVE SUMMARY

Executive Summary

Introduction

Since the publication of the National Cyber Security Strategy (NCSS) there has been a significant increase in malicious cyber activity globally from hostile nation states and cyber criminals. As our reliance on connected technology grows, the opportunities for those who seek to attack and compromise our systems and data will continue to increase, along with their potential impact on individuals, organisations and the wider economy.

That is why cyber security remains a top priority for the government - it is central not only to our national security but also fundamental to becoming the world's best digital economy.

A cyber security capability gap

Over the first two years of the NCSS we have engaged extensively with industry, professional organisations, students, employers, existing cyber security professionals and academia to better understand the nature of the cyber security skills challenge. We consistently hear that employers struggle to recruit individuals with the skills they need, or that there is a premium on appropriately skilled staff which some organisations struggle to afford.

To explore this demand for capability further, government commissioned research to define the basic technical cyber security skills gap. The study found that more than half of all businesses and charities (54%) have a basic technical cyber security skills gap, falling to 18% in public sector organisations.[1] Given the inherent nature of cyber threats to a digital economy, such a capability gap is not sustainable.

Yet we know that cyber security capability is much more complex than simply the number of cyber security professionals - it is about the level and blend of skills required across the economy, which will continue to evolve apace with technological advancements. New and emerging technologies, such as artificial intelligence, machine learning, and the proliferation of the Internet of Things will make this challenge more acute. Alongside the need for skilled cyber security professionals, digital literacy (in which cyber security is paramount) will undoubtedly become a more structured facet of a wider range of roles, in the same way as basic financial or commercial literacy is fundamental to most jobs in most sectors. Government and partners across the cyber security community must therefore work collaboratively to address these challenges to ensure that the UK has the cyber security capability it needs to maintain its resilience to increasing cyber threats.

Our Mission

This initial strategy adopts the strategic outcome set out in the NCSS - to ensure that 'the UK has a sustainable supply of home-grown cyber skilled professionals to meet the growing demands of an increasingly digital economy, in both the public and private sectors, and defence'. But it seeks to go much further.

Our ambition is to address the broader cyber security capability gap: ensuring the right skilled professionals are in the workforce now and in the future; ensuring that organisations and their staff are equipped to manage their cyber risks effectively; and ensuring that individuals have an understanding of the value of their personal data

and are able to adopt basic cyber hygiene to keep themselves and the organisations they work for protected.

Our mission is therefore to increase cyber security capacity across all sectors to ensure that the UK has the right level and blend of skills required to maintain our resilience to cyber threats and be the world's leading digital economy.

We will pursue this mission by working toward the following objectives:

1. To ensure the UK has a well structured and easy to navigate profession which represents, supports and drives excellence in the different cyber security specialisms, and is sustainable and responsive to change
2. To ensure the UK has education and training systems that provide the right building blocks to help identify, train and place new and untapped cyber security talent
3. To ensure the UK's general workforce has the right blend and level of skills needed for a truly secure digital economy, with UK-based organisations across all sectors equipped to make informed decisions about their cyber security risk management
4. To ensure the UK remains a global leader in cyber security with access to the best talent, with a public sector that leads by example in developing cyber security capability

A Structured and Trusted Profession

Cyber security is a broad and varied discipline that has grown rapidly and organically in recent years. This rapid development has led to a fragmented narrative around cyber security skills and a lack of coherence between the different specialisms. The absence of clearly established career and training pathways has meant that cyber security can be a confusing landscape to navigate, compounding the diversity challenges evident across the workforce.

A clear definition of cyber security skills

This initial strategy seeks to tackle these barriers by formulating a definition of what constitutes cyber security skills, acknowledging the broad range of aptitudes and skill-sets that are in demand across the economy. Recently commissioned research into the range of technical and non-technical cyber security skills suggests that the skills all organisations need are a combination of essential and advanced technical expertise, strategic management skills, planning and organisation skills, as well as complementary soft skills (see 'Defining Cyber Security Skills').

Defining Cyber Security Skills

We define cyber security skills as the combination of essential and advanced technical expertise and skills, strategic management skills, planning and organisation skills, and complementary soft skills that allow organisations to:

- Understand the current and potential future cyber risks they face
- Create and effectively spread awareness of cyber risks, good practice, and the rules or policies to be followed, upwards and downwards across the organisation
- Implement the technical controls and carry out the technical tasks required to protect the organisation, based on an accurate understanding of the level of threat they face
- Meet the organisation's obligations with regards to cyber security, such as legal obligations around data protection
- Investigate and respond effectively to current and potential future cyber attacks, in line with the requirements of the organisation

This defines the core set of knowledge and skills that organisations need to either have within their workforce, or seek externally (for example, if they outsource their cyber security or take on external consultants). Those working in the wider cyber security industry – developing cyber security products or services, or carrying out fundamental research – may require additional skills, such as the technical expertise and skills needed to research and develop new technologies, products or services.[2]

To build on this, the government has commissioned a team of UK academics to develop a Cyber Security Body of Knowledge (CyBoK) that will seek to define the foundational knowledge upon which the field is built.[3] We will publish the complete CyBoK in 2019.

An independent UK Cyber Security Council

But this in itself isn't enough. Our ambition is for there to be a new, independent UK Cyber Security Council that will embolden the profession to structure and develop itself in a way that meets current and future demands. The Council will be charged with the development of a framework that speaks across the different specialisms, setting out a comprehensive alignment of career pathways, including the certifications and qualifications required within certain levels. The Council will lay the structural foundations of the cyber security profession that will enable it to respond to the evolving needs of industry and the wider economy.

A Vibrant Education and Training Ecosystem

While providing the structural foundations of the profession is fundamental to its sustainability, there is a pressing need to take immediate steps to address the current cyber security capability gap, as well as ensuring the building blocks are in place for the future.

Inspiring the current workforce to retrain or upskill

To address the immediate cyber security skills shortages and bring a broader and more diverse range of skills and experiences into organisations, government has sought to boost the provision of cyber security retraining opportunities. Recognising the range of excellent, industry led initiatives that exist already, the government will continue to support the development of a vibrant industry led

training ecosystem. This includes the continuation of the Cyber Skills Immediate Impact Fund (CSIIF) in 2019/20 as well as exploring other ways of government helping to boost cyber security retraining provision.

Inspiring future cyber security professionals

To deliver a sustainable and lasting improvement to capability, it is also crucial that we take steps now to establish and develop the building blocks for future careers in cyber security.

Schools

The number of students taking computer science GCSE and A level qualifications in England has grown over recent years but take-up and availability still lags significantly behind other science, technology, engineering and mathematics (STEM) subjects. High quality teaching is essential to addressing this and the Department for Education is making significant investment in a new National Centre for Computing Education and associated prorgrammes that will continue to improve the expertise of all teachers of computer science. This investment is supported by the efforts of other initiatives, such as the National Cyber Security Centre's (NCSC) Cyber Schools Hubs programme in England which promotes cyber security educational resources to support teachers in the local community.[4] We will continue to support initiatives that seek to encourage the uptake of computer science GCSE and A level, including the potential expansion of NCSC Cyber Schools Hubs across England. There is a similar focus on qualifications in the devolved administrations, for example in Scotland there will be a continued roll out of school age qualifications in cyber security.

Further and higher education

Further and higher education programmes, including apprenticeships, are crucial platforms for converting talent into cyber security jobs. Apprenticeship schemes, such as the Critical National Infrastructure Apprenticeship scheme that the Department of Digital, Culture, Media and Sport (DCMS) has been piloting in collaboration with industry for cohorts recruited in 2017, support those working towards a qualification by providing the opportunity to gain real and practical skills, while undergraduate degrees provide the more traditional entry point to professional work. To facilitate this route to entry the NCSC, in partnership with industry, will continue to deliver a CyberFirst Bursary Scheme to provide undergraduates with financial assistance and cyber security work experience, while certifying a number of degree programmes to signpost high quality degrees for those who are interested in pursuing a career in cyber security.

To make the most of the highest levels of academia, we will continue to support the next generation of Centres for Doctoral Training in Cyber Security, building on the success of the two established in 2013, which will support students undertaking a doctoral programme. We will also continue to work with universities across the UK to directly support doctoral study in areas of strategic interest.

We are conscious, however, that not all cyber security roles are technical in nature and we propose to do more to capture those with the aptitude and skills that are in equally high demand. We will therefore explore how government and industry can attract new and untapped talent to careers in cyber security, to boost the numbers and diversity of those entering the workforce.

Extra-curricular

While formal education pathways play a significant role in providing young people with the building blocks they need to build a career in cyber security, there are activities outside of the classroom that can be more inspiring, especially to those who don't thrive in a formal environment. Our flagship £20 million Cyber Discovery programme, for example, aims to capture the imagination of young people and inspire them to consider a career in cyber security, while identifying and nurturing promising talent from a young age.[5] There are also many excellent industry and wider cyber security community led extra-curricular activities, including the cyber security curricula for 14-18 year olds run by University Technical Colleges in England, and Cyber Girls First - an initiative for 11-14 year old girls to learn more about online safety, cyber security and coding, and to meet female cyber security professionals.

We will continue to invest in and support such extra-curricular activities to inspire young people of school age across the UK to be aware of and consider a career in cyber security. To capture previously untapped talent pools we propose to support additional extra-curricular activities for 14-18 year olds that develop non-technical cyber security skills, as well as an extra-curricular learning platform for young people aged 5-14.

Providing greater coherence

We recognise that greater coherence and coordination to the range of initiatives that are offered across government is urgently needed. To achieve this we recently completed a review of the CyberFirst brand to enable us to unify all existing and potential initiatives under a single banner that appeals to all ages and experience. We will launch the refreshed CyberFirst brand in 2019 which will bring greater coherence to the government's offering on cyber security skills for all age groups. We will also continue to encourage industry to use CyberFirst content to deliver additional events and further boost the provision of extra-curricular initiatives.

As well as being able to access initiatives, we also know that to successfully capture future talent we need to make sure that potential cyber security professionals are informed about the different types of cyber security roles available and the career pathways that they need to take to get there. While the UK Cyber Security Council will lead on this in the future, there is much we can do in the interim.

We therefore propose to take decisive action to 'demystify' cyber security careers by beginning a programme of work in January 2019 to map the different career options and pathways and ensure there is clear and accessible advice for anyone who has the aptitude for a career in cyber security. This will align with and complement existing work in devolved administrations. We also propose to appoint one or more independent Cyber Security Skills Industry Ambassadors to help promote careers in cyber security to a broader and more diverse range of individuals across the UK.

Broader Cyber Security Capability for a World Leading Digital Economy

While the development of the cyber security profession and a vibrant education and training ecosystem are fundamental to meeting the current and future need for cyber security professionals, they are not enough to maintain the security and resilience of the wider digital economy. Cyber security cannot and should not be the responsibility of cyber security professionals alone.

To address the cyber risks inherent to an increasingly digital economy and society, as well as skilled professionals there must also be a general foundation of cyber security understanding embedded across the workforce and general population. Digital literacy, in which cyber security is implicit, must become universal.

Embedding basic cyber security universally

The government is introducing an entitlement to full funding for basic digital courses from 2020, to ensure that everyone, no matter what age, ability or background, has the opportunity to develop the skills they need to be safe and responsible online, and to protect their devices and data against common online risks and threats.

This need for digital skills is recognised within formal education, both through computer science and the forthcoming introduction of T Levels in England; technical qualifications in which digital skills are embedded throughout, alongside numeracy and literacy. We will also continue to support industry partners, such as the Institute of Coding and the Ada National College for Digital Skills, to provide courses and training at various levels up to degree standard, and will promote the expansion of initiatives that seek to upskill the current workforce; for example through the work of the Digital Skills Partnership (DSP) which brings together organisations across all sectors to tackle the digital divide.

Embedding cyber security within professional decision making

It is also important that those who require cyber security services, from small business owners to operators of critical services, have the knowledge and understanding they need to manage their cyber risk in a proportionate way, which includes making decisions on the professional cyber security services they require. Not only will this have a direct impact on any cyber security skills shortage, by helping to focus the scope of the services required, it will also ensure that cyber risks are being managed in an informed and appropriate way.

To support this the NCSC will continue to provide a plethora of simple and targeted guidance and tools, as well as operating their 'Cyber Essentials' certification scheme which is being strengthened to ensure that it is having the greatest impact. DCMS is also considering how the government can further equip organisations to make informed decisions, as well as how best to incentivise more proactive cyber risk management across the economy.

Embedding cyber security within professional disciplines

We must also strive to ensure that cyber security is prioritised and embedded, not only in the design and development of technology, but within professional disciplines across all sectors of the economy - just as a civil engineer is implicitly concerned about the integrity of a bridge, a software designer should be concerned about the integrity and security of software, and a bank should be concerned about the protection of the vast amount of private information it holds. These considerations are, and will continue to become, so increasingly important that they must be integrated into the disciplines that will require them.

The UK Cyber Security Council will, in time, seek to develop stronger links with other professions and disciplines across all key sectors to inform cyber security expectations that should be embedded within respective professional codes of conduct. In the interim we propose to explore with other professions how to begin to embed cyber security within relevant professional codes of conduct or codes of ethics to affect the necessary culture change.

Devolved administrations are also seeking to create context-free cyber resilience national occupational standards that can be used to embed cyber resilience in workers' roles across all sectors.

Leading the Way

We must work to ensure that the UK is the best place in the world to be a cyber security professional, to attract and retain the best from the rest of the world. The public sector has an important role to play in setting the example for other sectors across the economy.

The public sector leading by example

The public sector must aspire to set a clear example of the importance of investing in cyber security professionals. We will therefore increasingly focus on upskilling the public sector workforce, from board level to administrative assistants, in order to keep our systems and data safe.

By investing in our people, alongside our systems, we want to demonstrate that cyber security, and a cyber secure workforce, is one of our highest priorities. We will therefore provide increasing focus on the cyber security capability of the public sector to ensure that infrastructure, services and assets are protected, with the aspiration of being an exemplar for other sectors across the economy.

Engaging globally

Creating this environment and attracting and retaining the best cyber security talent is central to making the UK the world's leading digital economy. We are already recognised globally as a leader in cyber security and have a thriving and vibrant cyber security sector. We want to maintain that status and influence, and to work with other nations and multilateral institutions to operate effectively across defence and security, and to maintain a free, open, inclusive and secure cyberspace.

This is why we will continue to lead and participate in a range of international cyber security programmes and initiatives, such as the European Cyber Security Challenge and the UK/US Future Cybersecurity Leaders Exchange (an exchange which provides a hands-on introduction to a range of cybersecurity challenges). Participation in such initiatives will continue to strengthen the UK's global reputation, enable us to share best practice with our allies, and to collectively create a stronger and more digitally secure world.

Delivering in Partnership

Collaboration lies at the heart of success. Successes to date have been driven by close working between government and partners across the cyber security community. Continuing this collaborative approach is crucial. We must therefore build on this by expanding industry involvement in government initiatives while continuing to use government levers to support innovation.

The transformative investment of the National Cyber Security Programme (NCSP), which underpins the NCSS, is about building the foundations for a sustainable future. The NCSP comes to an end in 2021. While government will continue to support and drive the long term delivery of our objectives, we must work with the cyber security community to ensure that the range of required initiatives are sustainable. This may include the exploration of additional or alternative funding streams.

Ultimately, we need to continue to work in partnership to ensure that the capability gap is reduced, both now and in the future, to maintain the resilience of the digital economy.

Taking this Forward

Publication of this initial strategy introduces a ten week call for views - providing all those with an interest in cyber security the opportunity to engage and help shape and refine it.

We have set out a number of questions for readers to formally respond to and in parallel we will be running a series of engagement events across England and the devolved administrations in early 2019. Evidence from this call for views will help formulate a final strategy which we intend to publish later in 2019.

Endnotes

1 Pedley, D., McHenry, D., Motha, H., Shah, J (2018). Understanding the UK cyber security skills labour market. Ipsos MORI

2 Pedley, D., McHenry, D., Motha, H., Shah, J (2018). Understanding the UK cyber security skills labour market. Ipsos MORI

3 Cyber Security Body of Knowledge

4 Cyber Schools Hub

5 Cyber Discovery