



HM Government

INITIAL NATIONAL CYBER SECURITY SKILLS STRATEGY

INCREASING THE UK'S CYBER
SECURITY CAPABILITY

A CALL FOR VIEWS



Contents

Ministerial Foreword	3
Chapter 1 – Introduction	5
Chapter 2 – Strategic Context	8
Chapter 3 – The National Response: Our Mission	16
Chapter 4 – A Structured and Trusted Profession	19
A clear definition of cyber security skills	20
An agreed body of knowledge for cyber security	20
UK Cyber Security Council	21
Chapter 5 – A Vibrant Education and Training Ecosystem	25
Inspiring the current workforce to retrain or upskill	25
Inspiring future cyber security professionals	28
Chapter 6 – Broader Cyber Security Capability for a World Leading Digital Economy	40
Embedding basic cyber security universally	40
Embedding cyber security within professional decision making	42
Embedding cyber security within professional disciplines	43
Chapter 7 – Leading the Way	46
The public sector leading by example	46
Engaging globally	51
Chapter 8 – Delivering in Partnership	54
Chapter 9 – Implementation and Measuring Impact	56
Chapter 10 – Taking this Forward	59
Endnotes	63

Ministerial Foreword



MARGOT JAMES MP
MINISTER FOR DIGITAL AND
THE CREATIVE INDUSTRIES

The UK is a global leader in cyber security. We have a vibrant and growing cyber security sector with huge expertise and some of the most creative and innovative companies in the world. This is central not only to our national security, but also in realising the government's ambition to make the UK the safest place in the world to be online and the best place in the world to start and grow a digital business.

At the heart of the UK cyber security sector's success is people. The UK already has some of the best cyber security professionals in the world and a core part of the five year National Cyber Security Strategy is about further developing that talent. We have set in motion a series of major interventions to boost the number and diversity of cyber security professionals in the UK. This includes investing £20m in the flagship Cyber Discovery programme, which 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. We also continue to develop the CyberFirst initiatives right across the skills pipeline and have launched the Cyber Skills Immediate Impact Fund (CSIIIF).¹

However, as our digitally connected world has expanded at an extraordinary rate, so too has the scale of vulnerabilities and the frequency of attacks that we face. The threat has developed significantly even since the publication of the National Cyber Security Strategy in 2016. Public and private

sector organisations worldwide are falling victim to ransomware attacks, supply chains are being compromised and our critical national infrastructure continues to be a target for attack. We are also seeing threats to our democracies from attempted outside interference.

This brings in to even sharper focus the need to develop our people and have the right blend and level of skills. That is why I am so pleased to be publishing this Initial National Cyber Security Skills Strategy that builds on what we have already achieved and sets out a bold and ambitious approach to developing the right cyber security capability in the UK now and in the long term. This goes further than simply increasing the number of cyber security professionals in the UK. It recognises that cyber security is the responsibility of all of us, and of every organisation.

The approach proposed in this document is based on research and extensive engagement with the cyber security community over the last two years. But government does not have all of the answers - this is a complex challenge that requires us to further harness the expertise, creativity and innovation so evident in the UK cyber security community. That is why we are publishing this initial strategy with a call for views to give you the opportunity to engage in a meaningful way and help refine and iterate the approach set out.

This document defines a series of questions to respond to and in parallel we will run a series of events around the UK to explore the themes in this initial strategy further. We will then use the evidence to publish a finalised strategy. I hope as many of you as possible will engage and I look forward to hearing your views.

Chapter 1

Introduction

Chapter 1 – Introduction

The five year National Cyber Security Strategy (NCSS), published in 2016, set out the government's plans to make the UK secure and resilient in cyberspace, prosperous and confident in a digital world. It is backed with £1.9 billion of investment to help in defending our systems and infrastructure, deterring our adversaries, and developing a whole society capability.

There has been significant progress in delivering the NCSS, including the establishment of the National Cyber Security Centre (NCSC) to help protect our critical infrastructure and services from cyber attacks, manage major incidents, and improve the underlying security of the UK Internet. But since the publication of the NCSS, there has also been a significant increase in malicious cyber activity globally, from hostile nation states and from cyber criminals. As our reliance on technology grows, the opportunities for those who would seek to attack and compromise our systems and data will continue to increase, along with their potential impact.


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 core part of our response is ensuring the UK has the right blend and level of cyber security capability across our economy.

This Initial National Cyber Security Skills Strategy sets out a bold and ambitious approach to deliver that. It comes mid way through the implementation of the National Cyber Security Programme (NCSP)

and has at its foundation the range of policies and initiatives which have already been delivered or are in progress to boost the UK's cyber security capability and deliver on the outcomes set out in the NCSS. It also sets out, based on research and extensive engagement over the last two years, the government's understanding of the strategic context on cyber security capability and our vision and plan to develop the UK's cyber security capability now and in the longer term.

The challenge on cyber security capability is complex. Global and domestic market insight reports regularly refer to an unmet demand for cyber security capability. This initial strategy explores how this is felt across different parts of the economy in the context of the wider cyber threats we face as a country, as well as our understanding of the range of factors contributing to the cyber security capability gap. The challenge is much more complex than simply a shortage of cyber security professionals - there is a broader cyber security capability gap in the UK.² This is about the level and blend of expertise and skills needed across the general workforce to help the UK become the world's best secure digital economy.

The successes so far in delivering against the NCSS have been driven by close working between government and partners across the cyber security community. Continuing that collaborative approach is crucial and there is clear passion, enthusiasm, and a depth of expertise across all parts of the cyber security community which we need to harness.



We believe that making things open makes things better, and we want anyone with an interest to engage and meaningfully contribute to the strategy to develop the UK's cyber security skills and capability. The publication of this initial strategy introduces a ten week call for views. We have defined a series of questions to formally respond to and we intend to run a series of engagement events in early 2019 to explore these questions further.

Through the questions we seek to validate our assessment of the cyber security capability landscape and identify where there may be additional or further challenges in specific parts of the economy. We also seek to understand whether or not the level of ambition articulated through the mission and objectives is sufficiently ambitious to meet the challenge. To build on

our recent consultation on developing the cyber security profession and CyBOK consultations, we ask whether the definition of cyber security skills set out in this initial strategy reflects the consensus view in the UK cyber security community. We also set a series of questions about the proposals on interventions in the education and training ecosystem and how government and industry can work together to develop creative and innovative ideas to increase cyber security capability in the UK.

We are keen for as broad a range of responses as possible - there will be engagement events across England and in each of the devolved administrations. Responses to the questions should be made using the online portal and details of how to sign up for the events will be available through GOV.UK.

Chapter 2

Strategic Context

Chapter 2 – Strategic Context

Overview

This chapter sets out the government's understanding of the challenge on cyber security skills. This is a complex challenge. Cyber security capability is more than simply the number of cyber security professionals - it is about the level and blend of skills required across the economy. This chapter sets out the threat landscape and why the pace of technological change and the importance of security in new technologies makes this challenge even more pronounced.

Since the government published the National Cyber Security Strategy in 2016, the cyber threat has continued to diversify and grow. In the two years since the NCSC was created it has dealt with well over 1,000 cyber security incidents. In 2017, over 70% of large businesses, 64% of medium businesses and 42% of micro/small businesses in the UK suffered a cyber breach.³

The nature of the threat is evolving too; the NCSC believes the majority of the incidents they dealt with in 2017 were perpetrated from within nation states in some way hostile to the UK, meaning they were undertaken by groups of computer hackers directed, sponsored or tolerated by the governments of those countries.⁴ The commoditisation of small scale and less sophisticated attacks also means that even actors with low capability can have an impact.

Focus on: Cyber security risks - understanding the threat

The cyber threat to UK is significant and growing. Cyber threats are becoming increasingly varied and adaptive – ranging from high volume, commoditised and opportunistic attacks to highly sophisticated and persistent threats involving bespoke malicious software designed to compromise specific targets.

The increasing digitalisation of our economy and society compounds this challenge, as our dependency on connected devices and services further increases the potential vulnerabilities that can be exploited.

The make-up of attackers is also varied – from state sponsored actors to cyber criminals, ‘hacktivists’, or the actions of employees, whether deliberate or accidental. Most common of all is from cyber criminals seeking to exploit UK organisations for financial gain – whether that be the sophisticated theft of intellectual property or a simple theft of cash from an account. The rise of ransomware is particularly notable and is having a significant impact both to private businesses and public bodies.

Cyber threats pose a risk to organisations of all sizes and across all sectors, as well as public bodies and critical services.

As we increasingly move more of our daily lives and business online, and as we face an increasingly sophisticated level of threat from our adversaries, cyber attacks are unfortunately inevitable. It is critical that there is the cyber security capability across the economy to ensure that organisations take an informed and proportionate approach to cyber risk management which focuses on resilience, minimising the impact of attacks as and when they do occur.

Given that the threat itself is constantly and rapidly evolving, policy on cyber security skills must be similarly agile and dynamic. This means it is essential that training and skills development – across all sectors – is grounded in an accurate and up-to-date understanding of the threat.

These breaches come with a cost - both financial and/or reputational. We know that only 27% of UK businesses and 21% of charities have a formal policy or policies covering cyber security risks⁵ and many organisations lack the knowledge, understanding and confidence around cyber security to implement appropriate measures.⁶ Risks are regularly downplayed and businesses too often only take protective action after their systems have been breached or they have suffered an attack.⁷

This is a challenge for individuals, the public and private sectors alike. The government, public sector, charities and private businesses are all having to rapidly adapt their behaviours and practices to protect themselves and their

customers against this changing cyber threat. New legislation, such as the Data Protection Act 2018 and the Network and Information Systems (NIS) Regulations 2018, make it even more crucial that organisations have a firm grasp of their cyber risk management and can effectively protect themselves and their customers.

Beyond that, new and emerging technologies make this need even more pronounced. The proliferation of the Internet of Things (IoT) means consumers are bringing more and more internet connected devices into their homes, such as smart TVs, smart music speakers, smart washing machines, and even internet connected toys. Furthermore, tools for processing and making sense of large quantities

of data have developed exponentially, with artificial intelligence (AI) representing the latest leap. The AI Sector Deal⁸, published in April 2018, sets out the huge benefits and potential of AI and how this technology can transform how we diagnose diseases, manufacture goods and build our homes.

However, with these benefits come associated risks. If internet connected devices sold to consumers lack even basic cyber security provisions, people's privacy and safety is at risk of being undermined. Additionally, the wider economy faces an increasing threat of large scale cyber attacks - for example a coordinated attack on IoT devices that are part of a smart city could affect electricity supplies far beyond individual homes. Part of how we harness AI and other technological advancements to get the maximum benefit from them is about ensuring they develop securely by design. Having the right capabilities, capacity and professionalism in our cyber security workforce now and in the future is fundamental to that.

Since the publication of the NCSS we have engaged extensively with industry, professional organisations, students, employers, existing cyber security professionals and academia to better understand the nature and nuances 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 for appropriately skilled staff which some organisations struggle to afford.

This is a complex challenge, with a range of issues and causes amplifying one another and combining to make the overall challenge more acute and pronounced. This includes definitions of what we mean when we speak about cyber security, unclear pathways into a career in cyber security, diversity and inclusion, and the changing nature of the general workforce. Underlying all of this is a need for cyber security capability which better meets the demand in an effective, secure digital economy.

A capability gap

There has been a range of research conducted globally which has sought to quantify the shortage of cyber security professionals. The most recent (ISC)² global study, for example, sets out that there is a shortage of 2.93 million cyber security professionals internationally.⁹ While this gives some sense of the global nature of the challenge on cyber security skills, cyber security capability is more complex than simply the number of cyber security professionals.

Capability is about the level and blend of expertise and skills needed to help the UK become the world's best and most secure digital economy. Indeed, cyber security is a fast moving and ever-evolving area with a shortage of wholly accepted and adopted definitions - we therefore believe it would be inherently challenging to accurately define the size of the shortage of cyber security professionals in the UK. Nor would producing a headline number recognise the multidisciplinary nature of cyber security as a domain with a number of specialisms, or the fact that for many, cyber security is a small part in a wider role rather than a distinct role in itself.

Indeed, there are many widely recognised cyber security roles, from technical roles like penetration testing and cryptography through to the more strategic positions of Chief Information Security Officers. For many, cyber security is a technical domain and for others it is more strategic or policy focused. We have heard from a range of stakeholders about challenges in recruiting for all of these roles and the fact that organisations in different parts of the economy experience the capability gap differently and have different ways and means of addressing it.

Rather, we have sought to better understand the nature and nuances of the demand and supply to give us a more comprehensive picture of where the capability gap is felt. This demand for more cyber

security capability spans both public and private sectors. Traditionally, careers in government have been one of the main pathways for cyber security talent, with strong demand for a range of technical and non-technical cyber security professionals to work in national security in the intelligence and military community and more broadly across the public sector, such as in the NHS, to protect citizens' data. Increasingly, however, sectors like finance, retail and charities have demands for cyber security professionals which we expect will continue to grow.

The demand is not simply for cyber security professionals either. Responsibility for cyber security goes far beyond that - almost every individual and every part of an organisation has a role to play. The general workforce's digital literacy and understanding of cyber security will continue to grow in importance, as will the requirement for other professions and sectors to have a more well defined focus on cyber security. We believe cyber security will become a more structured facet of a wider range of roles, in the same way as basic financial or commercial literacy is a part of most jobs in most sectors. This will address the root cause and potentially change the nature of specialist cyber security.

To explore this demand for capability further, government has commissioned research to define the basic technical cyber security skills gap. It identified skills areas based on the five technical controls within the Cyber Essentials scheme (for example securing devices and software, and controlling who has access to the organisation's data and devices)¹⁰ and two other basic aspects of cyber security beyond this: storing or transferring personal data securely, which is a requirement of all organisations under the General Data Protection Regulation (GDPR), and backing up files and data.

More than half (54%) of all businesses and the same proportion (54%) of charities have a basic technical cyber security skills gap. For public

sector organisations, 18% have a basic technical skills gap.¹¹ Consequently this means that of the c.1.32 million businesses in the UK, approximately 710,000 have a basic technical cyber security skills gap, of the c.199,000 registered charities approximately 107,000 have this gap, and for the c.12,400 public sector organisations approximately 2,200 have this skills gap.¹²

In the private sector, basic technical skills gaps tend to be more prevalent in sectors such as food or hospitality, whereas, perhaps unsurprisingly, there is less of a gap in the information or communications, and finance or insurance sectors¹³. For more high-level technical cyber security skills¹⁴ the skills gaps are higher in the private sector than in the public sector (31% of businesses have a high-level technical skills gap, 22% of charities and 27% of public sector organisations).¹⁵ It is estimated that 407,000 businesses have a high-level technical skills gap and 43,700 charities and 3,300 public sector organisations have a high-level technical skills gap.¹⁶ Technical skills gaps tend to be higher outside the finance or insurance sectors and the information and communications sectors, as well as outside of London.¹⁷

The vast majority of those with cyber security responsibilities across businesses, charities and the public sector have absorbed them into their existing non-cyber security jobs. Consequently, outside of the external cyber security providers,¹⁸ they are often not labelled as working in 'cyber' roles - just 11% of businesses and 14% of charities on average have cyber security written formally into the job descriptions of one or more staff.¹⁹

Many organisations choose to outsource their requirement for cyber security capability. Three in ten businesses (30%) and a similar proportion of charities (27%) outsource one or more aspects of their cyber security, while public sector organisations are more likely to outsource, with two thirds (65%) doing so.²⁰ Among organisations that do outsource cyber security, most still handle

at least some aspects in-house, and while public sector organisations are more likely to outsource some cyber security activities, their level of outsourcing is more likely to be light touch, with more aspects typically handled in-house than in businesses and charities.²¹

While outsourcing is not in itself problematic, there still needs to be some capability in-house to set the requirements, make informed choices and ensure the contracted resource is effective. Anecdotally we have heard that many, particularly small and medium businesses, rely on informal networks and word of mouth to find a provider.

Definitions and a new profession

There are a number of underlying reasons for the capability gap. Part of this is a lack of clear definitions and parameters of cyber security, which mean it can be difficult for organisations to articulate in a consistent way their demands or shortages. Cyber security is still a relatively new area which has developed rapidly and organically over recent years. The understanding of what constitutes a cyber security professional varies - those working in cyber security are found across multiple disciplines with a wide range of different competencies.

We know that cyber security roles within organisations are often not badged as 'cyber' roles. Indeed, cyber security is most often managed on an informal basis across organisations - the vast majority of individuals who have some responsibility for cyber security within their organisation do not have formal qualifications and are not working towards them either. Overall, 4% of businesses, 6% of charities and 19% of public sector organisations have individuals with or working towards relevant qualifications (this does not include cyber security external providers).²²

This has led to a fragmented narrative around cyber security skills and a lack of coherence between the different specialisms. The lack of clarity means

that for those considering a career in cyber security (either those new to the labour market or those retraining), it can often be a hard and confusing landscape to navigate with an absence of clearly established career and training pathways into and through the profession.

Beyond that, like in all sectors of the economy, the labour market is changing faster now than at any time in recent memory. Young people may, in the coming years, be doing jobs that those in the current labour market cannot yet conceive. Those working in cyber security are already having to deal with rapidly changing ways of working and further technological advances on the horizon will inevitably have an impact on the nature of the roles.

We know artificial intelligence and machine learning are already helping keep systems safer and more secure, but with the further development of that technology and the potential of quantum computing bringing even greater power to bear, the nature and way cyber security professionals work is likely to change at an even greater pace. For example, recent research has identified the area of automation, data analytics and threat hunting as key cyber security technical skills that will be required in the future alongside greater mathematical knowledge.²³

Building blocks in our education system

Currently cyber security is taught in both the higher and further education sectors within the UK, and as a discrete subject in schools in Scotland, either as a unique course or as a module within another course. However, it is often not widely available and the numbers of students participating in these courses or apprenticeships is often low.²⁴ Entry into both higher and further educational courses also often requires a science, technology, engineering and mathematics (STEM) qualification or background, thus cyber security courses are having to compete with other subjects and sectors to attract people with STEM skills.²⁵

In the further education (FE) space in 2016-17, there were over 47,000 students studying in ICT related fields with 670 students studying cyber security.²⁶ Currently (2017/18) there are 230 students who have started the level 4 Cyber Security Technologists apprenticeship and up to 10 students have started the Cyber Intrusion Analysts level 4 apprenticeship.²⁷

In the higher education (HE) space there are a total of 105 full-time courses in cyber security available at undergraduate and postgraduate levels in England, and a further 16 elsewhere in the UK.²⁸ The number of students undertaking cyber security related courses has steadily increased both at an undergraduate and postgraduate level (in the period 2014/15-2016/17 there was a 22% increase in the number of postgraduates and a 31% increase in the number of undergraduates).²⁹ However, in 2016-17 there were fewer than 6,000 HE students with a cyber security related degree.³⁰ In Scotland, there are 13 universities delivering at least 20 graduate level qualifications in cyber security. Scottish further education colleges are also delivering Higher National Certificates in Cyber Security with onboarding for the Higher National Diploma starting from summer 2019³¹, accompanied by shorter Professional Development Awards aimed at upskilling.

We know that computer science is a key enabler for entry level roles in security. Employers have highlighted, however, that they often have to look wider when recruiting entry level roles. They consider those with STEM backgrounds, with a particular focus on computer science, mathematics or engineering, as they often struggle to get students with the complex technical cyber security background required, and further upskilling is needed.³²

Consequently, this initial strategy lays out plans to ensure that the UK has an education and training system that provides the right building blocks to help identify, train and place new and untapped cyber security talent.

Cyber security in the workforce

As set out above, having an effective, secure digital economy is not the sole domain or responsibility of cyber security professionals. They have, and will continue to have, a key role to play, but embedding cyber security responsibilities in a broader range of roles is crucial if we are to meet the challenge and opportunities that technological change presents.

This starts with wider digital skills; ensuring that all citizens have the digital skills they need to be part of a digital economy and society. The younger generation are often more comfortable with digital technology, and alongside the strong foundation provided by the national curriculum and the fruition of some of the interventions outlined in this initial strategy, they will have a stronger understanding of cyber security. However, we know that there are many in the current workforce who do not have a strong enough grasp of the basics of cyber security hygiene practices.

We also know demand for cyber security capability is not always sufficiently well informed. Some organisations struggle to articulate their requirements. Senior leaders and boards have a significant role to play in resolving this issue. In many cases, they ultimately have responsibility for the organisation's approach to cyber security and therefore should have an understanding of the threats that their organisation could face and how to counter them. Ultimately, organisations can only attract the talent they require by understanding what they need in the first place.

Continued collaboration between government and all parts of the cyber security community is critical to increasing the UK's cyber security capability. The public sector needs to be an exemplar of best practice while being open to creative and innovative ideas and initiatives developed elsewhere. There are some excellent examples to build on, such as the NCSC's advice to organisations and individuals and the partnerships between academia, employers and government that are so critical

to developing a world class higher education sector in the UK. Government also needs to use its convening power to bring different parts of the cyber security community in the UK together to

collaborate and share best practice. We can also use our reach and networks to ensure the UK is well placed internationally to draw on best practice from around the globe.

Call for views

In this chapter we set out the government's understanding of the challenge on cyber security skills. We believe the challenge is a complex one which represents a cyber skills capability gap in the UK. Yet we know this is felt differently across different sectors and parts of the economy. We want to validate our assessment of the cyber security capability landscape and identify where there may be additional or further challenges in specific parts of the economy.

- To what extent do you agree with government's assessment of the strategic context?
 - Do you think there are any other challenges or issues that are not covered in the government's assessment of the strategic context?
-

Chapter 3

The National Response: Our Mission

Chapter 3 – The National Response: Our Mission

Overview

This chapter takes the NCSS strategic outcome as a starting point and sets out government's proposed longer term mission on cyber security capability as well as our proposed objectives for delivering that mission.

The NCSS's strategic outcome 9 sets out the aspiration 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."

The government has already made significant progress on cyber security skills and capability, delivering a range of initiatives designed to boost the number and diversity of those going in to cyber security careers. However, we recognise that, in view of technological advances and the changing and evolving threat landscape, we need to do more and go further. Our ambition is therefore to not only address the supply of cyber security professionals, but also to address the broader capability gap that is so fundamental to maintaining the resilience of our digital economy.

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

The NCSS set out a range of success measures around the profession and education system. Based on our close engagement with industry and partners across the cyber security community, and our ambition to address the broader capability gap, we have built on those to develop four new, clear cyber security skills objectives.

We believe these fully capture our intent and activity to deliver the strategic outcomes set out in the NCSS on cyber security professionals, while recognising that we need to do more to further embed cyber security capability within the UK's digital economy to ensure its continued security and resilience. The four objectives are:

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 to achieve a 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.

Call for views

This chapter sets out government's longer term mission on cyber security skills to increase cyber security capability across all sectors. It also defines four proposed objectives to deliver that mission. We want to understand whether or not the level of ambition articulated through the mission and objectives is sufficiently ambitious to meet the challenge.

- To what extent do you agree that the mission and objectives set out are sufficiently ambitious to address the challenges identified?
 - Why do you agree/disagree that the mission and objectives are sufficiently ambitious?
-

Chapter 4

A Structured and Trusted Profession

Chapter 4 – A Structured and Trusted Profession

Overview

While there has been significant progress to develop the cyber security profession in the UK, more needs to be done. The taxonomy around cyber security can be confusing and routes into and through cyber security careers can be hard to navigate. Addressing this to ensure there is a structured and sustainable cyber security profession in the UK is critical to our cyber security capability. This section sets out the decisive action being taken to develop a clear definition of cyber security skills, an agreed body of knowledge, and to create a new, independent UK Cyber Security Council as the focal point for the cyber security profession in the UK.

Objective 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

Cyber security is a broad and varied discipline that has grown organically and quickly in recent years. While progress has been made to ensure cyber security is a well structured and easy to navigate profession that drives excellence across the different specialisms, there remain challenges.

The definitions around what constitutes a cyber security role or skill are still developing and the concept of cyber security as a coherent profession is a relatively new one. For those working in cyber security and employers of cyber security professionals, the current qualification and certification landscape can be hard to navigate, making it difficult to assess the options available and to make appropriate, informed choices about career paths or the skills that an organisation requires. The technical language and acronyms which are often used can make this challenge particularly pronounced for those new to or unfamiliar with cyber security. The current professional landscape is also complex for existing professional organisations and vendors of cyber security qualifications and certifications, who are often unable to articulate the equivalence of their offerings in the absence of a common technical framework.

We believe the approach to tackling these remaining challenges and delivering the objective set out in this initial strategy has three main components. First, an agreed definition of what constitutes cyber security skills; second, an agreed body of knowledge for cyber security; and third, a well structured professional sector that works to effectively serve the interests of the cyber security community. Government has already taken decisive action to set in motion this activity. The sections below summarise that effort and set out what more government, working hand in hand with the cyber security community, intends to do.

A clear definition of cyber security skills

We are commonly asked about the definitions and parameters of cyber security when talking about developing skills and capability. The NCSS describes cyber security as *“the protection of internet connected systems (to include hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures or being manipulated into doing so”*.³³

Whilst this is an accurate definition of cyber security, it does not clarify the skills that will be required by individuals working in the different specialisms of cyber security. To address this, the government commissioned Ipsos Mori to conduct research³⁴ into the range of technical and non-technical cyber security skills in the workplace and to develop a clear definition of cyber security skills. They concluded:

“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

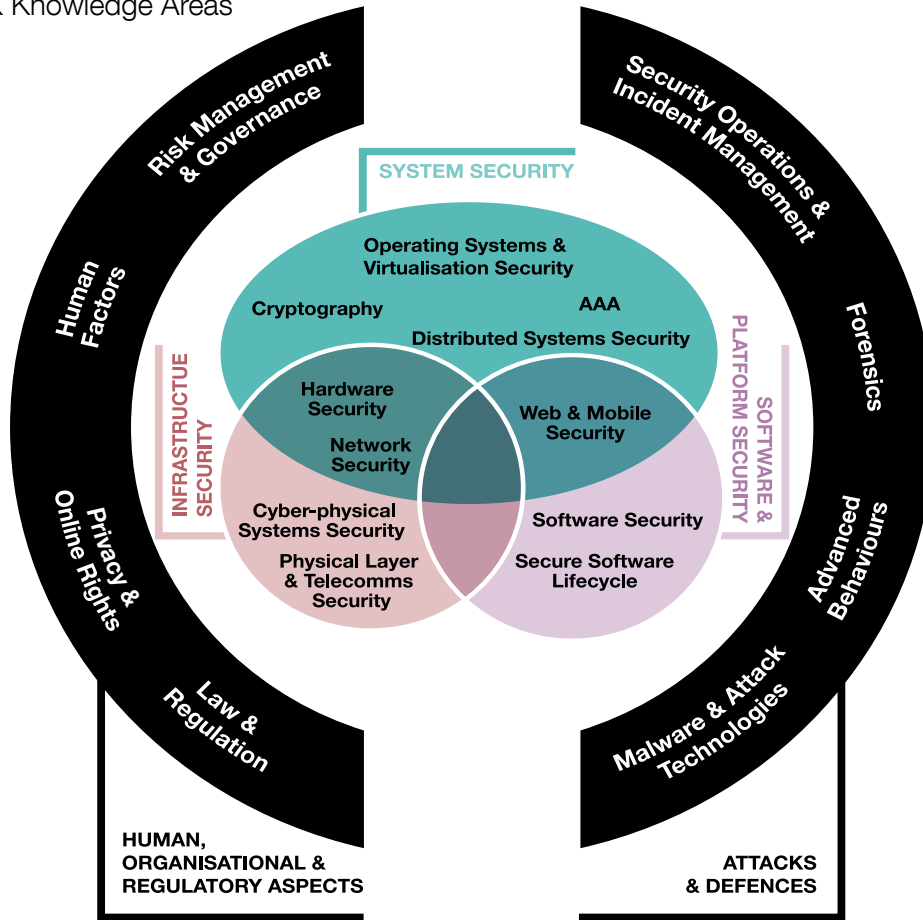
This defines the core set of knowledge and skills that organisations need to either have within their workforce, or seek externally (for example, if they outsource their cyber security or take on external consultants). Those working in the wider cyber security industry – developing cyber security products 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.”

An agreed body of knowledge for cyber security

To explore the parameters and breadth of cyber security in more depth, government has commissioned a project to define the foundational knowledge upon which the field is built. The development of the Cyber Security Body of Knowledge (CyBOK) is being undertaken by a team of UK academics, led by Professor Awais Rashid of Bristol University, in consultation with the national and international cyber security sector.

Phase One, completed in October 2017, focused on defining the scope of cyber security. In Phase Two, descriptions of the resultant 19 Knowledge Areas are being developed by experts from across the international cyber security community.³⁵

Figure 1: CyBOK Knowledge Areas



It is also worth noting there are already many and varied global initiatives to further describe and develop the domain. For example, in the US the National Institute of Standards and Technology (NIST) is leading the National Initiative for Cyber Security Education (NICE) which is focused on cyber security education, training and workforce development. Part of the work to deliver on this strategy will be to explore further how the outputs of the various initiatives align with the UK led CyBOK work.

Proposal 1

We will publish a complete Cyber Security Body of Knowledge, including all 19 Knowledge Areas, in 2019 to ensure there is an excellent foundation for professional standards in cyber security.

UK Cyber Security Council

The NCSS sets out a commitment to develop the cyber security profession in the UK and help it achieve Royal Chartered status. The intent behind this was to help ensure those working in cyber security can have their skills and expertise recognised more easily and in a clear and consistent way, as well as helping employers and consumers be more confident in the professionalism, capability and integrity of those they employ or those who provide cyber security services. It also sought to ensure the profession more coherently encourages a broader range of people with the right capabilities to enter the profession.

In summer 2018, government published a consultation which set out bold and ambitious proposals to implement the NCSS commitment

to develop the profession. The headline proposal was for there to be a new, independent, UK Cyber Security Council to act as an umbrella body for existing professional organisations and drive progress against the key challenges the profession faces. The consultation set firm deliverables for the Council, such as the creation and promotion of a new code of ethics for cyber security professionals.

We have now analysed the responses to the consultation. The government response³⁶, which is published in parallel with this initial strategy, sets out the strong support for the main thrust of the proposals. Government therefore now intends to proceed to identify a delivery lead to design, set up and implement the Council.

One of the key early requirements for the Council will be to develop a framework, agreed across the different specialisms, setting out the comprehensive alignment of career pathways through the profession, leading towards a nationally recognised career structure adopted by the whole cyber security sector across the UK. It will set out how certifications and qualifications relate to one another and link together. As part of that framework, we expect the Council to develop routes to Chartered Status for a new, commonly adopted 'cyber security professional' across all specialisms in cyber security. We believe this will help individuals and organisations make informed choices about the certifications and qualifications they require or should look for within certain levels.

In response to the public consultation we have further refined and prioritised other objectives for the Council to deliver. There was strong support for creating an agreed code of ethics across the different parts of the cyber security profession,

for example. This is an important early deliverable that will help drive up trust and expectations of professional conduct in cyber security and more broadly enable employers and consumers to be more confident in the professionalism, capability and integrity of those they employ or those who provide cyber security services.

Proposal 2

We will invest between £1m - £2.5m to establish a new, independent UK Cyber Security Council.

The newly formed UK Cyber Security Council will be charged with delivering an ambitious programme of work:

- Create a defined list of certifications and an easy to understand framework of how they all link together and what capabilities they convey, building on the career pathways work undertaken already
- Create a new code of ethics for cyber security professionals across all specialisms
- Develop and administer a Royal Chartered Status for cyber security professionals to aspire to
- Develop a robust roadmap for the Council becoming self-sustaining and fully independent of government

This process will begin with a competition to identify the delivery lead for the Council.

Call for views

This chapter sets out the decisive action being taken to develop a clear definition of cyber security skills, an agreed body of knowledge, and to create a new, independent UK Cyber Security Council as the focal point for the cyber security profession in the UK. We have recently consulted on developing the cyber security profession and CyBOK knowledge areas continue to be consulted on. We acknowledge, however, that there are still challenges around taxonomy and defining cyber security skills. We are therefore seeking to understand whether the definition of cyber security skills set out above reflects the consensus view in the UK cyber security community.

- Do you think there is anything missing from the definition of cyber security skills?
-

Chapter 5

A Vibrant Education and Training Ecosystem

Chapter 5 – A Vibrant Education and Training Ecosystem

Overview

The cyber security capability gap is both an immediate issue and a future concern. This chapter sets out the steps we will take to attract diverse talent into the profession by supporting opportunities to inspire the current workforce to retrain as cyber security professionals, as well as putting in place the building blocks for future careers in cyber security through formal educational and extra-curricular activities that will inspire future cyber security professionals. A key component of this is providing greater coherence and coordination to the range of initiatives that are offered.

Objective 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

The cyber security capability gap is both an immediate issue and a future concern. This means taking decisive action at all parts of the education and training ecosystem. To deliver a sustainable and lasting boost to capability, it is crucial that we take steps now to develop the building blocks for future careers in cyber security, ensuring that the talent and skill-sets are available to tackle the security challenges of the future.

This means ensuring that our education system provides genuine opportunities to learn and apply the foundational skills as well as supporting extra-curricular activities to inspire young people to pursue cyber careers.

In parallel, we also need to encourage and support adults who have the right aptitude, including those from non-traditional backgrounds, into cyber security careers. This requires a sufficiently vibrant cyber security training ecosystem that promotes routes of entry into cyber security jobs for a broader and more diverse range of individuals.

Inspiring the current workforce to retrain or upskill

While some specialist cyber security roles require a longer lead time and deeper technical expertise, retraining and career transition is a way to quickly fill many cyber security vacancies and bring a broader range of skills and experiences into an organisation. This might be in the form of retraining or upskilling existing staff in organisations, identifying individuals in other sectors who have the right aptitude and skills, or routing students coming out of university who are looking for a varied and fulfilling career into cyber security.

This is a well established model of entry in some other fields; there is a vibrant market of software developer retraining bootcamps in the UK, for example. There are a number of similar and excellent initiatives in cyber security. This includes an online platform to help further and higher education students get hands-on experience of cyber security and connect with prospective employers. There are also a range of initiatives to help veterans from the military develop the skills

needed to become cyber security professionals and a range of employer led in-house cyber training programmes to take new recruits from a range of backgrounds to quickly meet their cyber security capability needs.

These interventions are only possible through the partnership and collaboration of training providers, charities, academic institutions and industry. While this range of activity is positive, there is a need to further develop the training and retraining provision in the UK. Government wants to ensure that there are accessible and attractive opportunities for a much broader range of individuals to train and retrain.

In recognition of that need, the government has sought to support industry to help accelerate the

development of the cyber retraining ecosystem. Our key intervention in England is the Cyber Skills Immediate Impact Fund (CSIIIF) which is designed to provide funding and support to training providers and charities to run initiatives to quickly boost the number and diversity of those entering the profession.

The CSIIIF pilot launched in February 2018 and identified seven initiatives across England which would receive support to stand-up and scale-up. These initiatives are delivered through various methods, from face-to-face teaching to online platforms. Notable examples of sponsored projects include a 10 week retraining bootcamp for women and a neurodiverse community cyber security centre initiative.

CASE STUDY: Cyber Skills Immediate Impact Fund (CSIIIF) - Community Cyber Security Centre Pilot

A community based initiative proposed establishing a local cyber security training centre to identify, train and place unemployed neurodiverse individuals into cyber security roles. This centre was designed to provide a safe environment, focused on the needs of the trainees, where these individuals could relax, learn and discover their potential in the field of cyber security alongside designated mentors.

While there was interest from industry partners, initial investment from industry was difficult to obtain given this was an entirely new proposal. Through the CSIIIF, the proposal secured initial seed-funding that helped to establish the initiative - identifying a location and helping to purchase the infrastructure required to build an operational centre. This initial funding was provided on the basis that it would help to secure match funding from industry, to ensure that the project could become self-sustainable without long-term government funding.

The centre was set up rapidly over summer 2018 and has already helped 24 neurodiverse candidates get ready for a career in cyber security. There has been significant in-kind industry support to provide training platforms (including from other organisations sponsored by the CSIIIF) and career advice for participants. Crucially, the initiative has now received further funding from industry to establish a work experience programme for the neurodiverse candidates trained at the centre.

As CSIIIF continues to expand and sponsor new initiatives we will undertake a comprehensive evaluation of the Fund to ensure that the projects being funded are delivering the results that our industry partners expect. The outputs will directly

inform future industry-led interventions that will seek to continue to develop a cyber security retraining ecosystem and support a sustainable supply of cyber security professionals.

Proposal 3

We will continue to support the development of the cyber security training ecosystem through additional and more targeted government funding. This will include the continuation of CSIIIF in 2019/20 as well as exploring other ways of government helping to boost the cyber security retraining provision in the UK.

We will undertake a comprehensive evaluation in early 2019 of government interventions in cyber security retraining to inform our future approach. We will also work with devolved administrations to share best practice and consider wider roll-out.

As well as supporting training providers, we are also investing in a Cyber Security Postgraduate Bursaries Scheme to encourage adults to retrain by taking an NCSC certified Masters degree. Over three academic years, this scheme will support over 150 adults to retrain for a career in cyber security. There is activity across the whole of the UK - the Government of Northern Ireland and the Welsh Assembly, for example, are collaborating with industry to up-skill people in cyber security in preparation for employment by companies in the sector (see the 'Interventions being progressed by the devolved administrations' case study).

CASE STUDY: Interventions being progressed by the devolved administrations

Future Skills Cyber Security Fundamentals Academy (Government of Northern Ireland)

In preparing for the devolution of further fiscal powers to Northern Ireland, the Department for the Economy developed a Future Skills Cyber Security Fundamentals Academy in 2017, to support the recruitment of staff for Foreign Direct Investment or when a collaborative network of employers identify a particular skills need. The Academy is delivered by Belfast Metropolitan College for PWC and Black Duck Software.

Entry requirements promote applications by those that don't meet the academic criteria but are able to demonstrate technical skills and aptitude. 24 students successfully completed the 19 week Academy training and, to date, 13 have been offered employment with the participating companies.

The National Cyber Security Academy (Welsh Government)

The University of South Wales (USW) and the Welsh Government have joined forces to launch the National Cyber Security Academy (NCSA) to develop the next generation of cyber security experts. The NCSA, the first of its kind in Wales and a major UK initiative, is located in USW's Newport City Campus and offers the BSc (Hons) Applied Cyber Security.

With funding support from the Welsh Government, the NCSA is involving major industry players including Airbus, Alert Logic, QinetiQ, Wolfberry and the South Wales Cyber Security Cluster. Undergraduates work on real-world projects set by the NCSA partners who help to ensure the course meets the latest cyber security challenges.

It is our ambition to promote and progress the excellent work that is happening across the UK to attract and develop new talent and to support industry in taking on and sustaining these activities following the NCSP. These interventions are providing genuine routes to entry for many and are helping boost cyber security capability. However, we recognise that we need to continue this work, identifying new and creative ways to get a broader and more diverse range of people into cyber security, supporting efforts led by industry to retrain and upskill cyber security professionals across the UK.

Inspiring future cyber security professionals

Formal education provides the universal building blocks that will equip young people in pursuing careers in cyber security. Having access to high quality teaching of computer science in schools will lay the foundations that can be developed and practically applied in further and higher education, empowering people to take up more technical roles that are in such high demand. However, formal education is not the only vehicle for capturing and harnessing the imagination and talent of young people. Extra-curricular activities are a key way of identifying talent and feeding and developing interests at a young age, helping to develop skills and signpost future career paths.

We recognise that in order to successfully capture future talent we need to make sure that future 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 - from taking particular subjects at school or in further and higher education, or gaining relevant experience outside of the classroom. The Scottish Government, for example, have worked with their partners to develop a qualifications pathway from school through to university. In schools, students can study for National Progression Awards in Cyber Security, in colleges there are Higher National Certificates and Higher National Diplomas in Cyber

Security, and within higher education institutions students can undertake a range of Cyber Security undergraduate and postgraduate qualifications.

In time, the UK Cyber Security Council will take on responsibility for the development of an agreed framework of career pathways, including qualifications and certifications. However, we acknowledge that the Council will take some time to establish itself and there is work to be done in the interim to address this need.

Proposal 4

We will 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. The outputs of this work will be taken on and owned by the new UK Cyber Security Council.

Proposal 5

We will appoint one or more independent Cyber Security Skills Industry Ambassadors to help promote the profile, attractiveness and viability of a career in cyber security to a broader and more diverse range of individuals. We will work closely with industry partners to define the role(s) but one of the key functions would be to help distil and represent views of the cyber security community to government and vice versa.

Formal education - schools

A strong national curriculum is crucial, not only in providing young people with the initial building blocks required for more technical careers, but in developing broader digital skills which are increasingly vital to engaging and working in a digital economy.

Since 2014, computer science has been a statutory subject for 5-14 years in schools in England and provides a valuable foundation for computational thinking, creative problem solving and many other digital competencies. It is encouraging to see a growth in the number of students taking computer science GCSE³⁷ and A level³⁸ qualifications in England over recent years, but take-up and availability still lags significantly behind other STEM subjects.

High quality teaching is critical to achieving an increase in the number of pupils in schools and colleges who study towards computer science qualifications, particularly amongst girls and in disadvantaged areas. The Department for Education is making significant investment in order to continue to improve the expertise of all teachers of computer science in order to ensure all pupils have the digital skills they need for the future and that teachers are empowered to deliver excellence (see the 'Investment to improve the teaching of, and participation in, computer science' case study). Industry led programmes such as STEM Ambassadors are also doing excellent outreach work into schools to try and encourage STEM uptake.

The NCSC Cyber Schools Hubs programme aims to identify methods of building capacity and capability of cyber security educational resources to support teachers in the local community

in England. Local schools and their teachers, supported by the NCSC, have formed three pilot hubs using cyber security as a way to encourage a diverse range of students into taking up computer science, supporting students throughout the course and developing new content and resources to be made widely available for teachers. The hubs provide a potential blueprint for a scheme that could be implemented on a national scale to provide a local focus for cyber security resources as well as facilitate industry engagement.

Proposal 6

We will explore how to expand the NCSC Cyber Schools Hubs pilot across England.

A similar approach is being taken in the devolved administrations. In Scotland, for example, schools introduce the fundamentals of computer science, coding and digital skills from the early years onwards. Schools are supported to develop digital skills and learning across the Scottish curriculum by the Scottish education agency, Education Scotland, through its Digital Schools Programme, working in partnership with the British Computing Society and digital employers. Scottish schools have delivered National Progression Award qualifications in cyber security since 2015, with increasing numbers year-on-year.

CASE STUDY: Investment to improve the teaching of, and participation in, computer science

Backed by the £84m funding announced in November 2017, the Department for Education has launched a comprehensive programme to improve the teaching of computing and drive up participation in computer science, particularly amongst girls in England. This includes:

- A new National Centre for Computing Education, including a national network of at least 40 hubs to support schools to provide training and resources to primary and secondary schools
- An intensive Continuing Professional Development (CPD) programme of at least 40 hours for secondary school teachers. This will be designed for computing teachers without a post A level qualification in computer science and aims to reach up to 8,000 secondary teachers – enough for there to be one in every secondary school
- An A level programme supporting the delivery of A level computing to improve the quality of teaching, and increase students’ knowledge, skills and understanding, to better prepare them for further study and employment in digital roles

Formal education - further and higher education

Further and higher education provides opportunities to practically apply the building blocks taught at school and to develop skills that will be applicable in a work environment. This is the threshold into the profession and therefore a crucial stage in converting talent into cyber security jobs.

We have taken forward a number of interventions during the NCSP to support these opportunities. These include apprenticeships, which provide the opportunity to gain real and practical skills while working towards a qualification. Not only are they beneficial for the apprentice, but they offer organisations the opportunity to shape and teach technical skills that have real world application, directly addressing issues of real priority and significance.

Through the pilot Cyber Security Critical National Infrastructure Apprenticeship and the Government

Security Profession’s Cyber Security Technologist Apprenticeship schemes, hundreds of apprentices and employers are being supported as they progress through an 18 month to 2 year Cyber Security Technologist level 4 apprenticeship programme.³⁹ Launched in September 2018, the NCSC is also supporting 61 students through a three year Cyber Security Technical Professional Degree Programme, culminating in the award of Degree (level 6) apprenticeships.

In Scotland, there is a Modern Apprenticeship available in Information Security aimed principally at school leavers but also available to people of all ages. There is also a Graduate Apprenticeship in Cyber Security, currently provided at Bachelor and Masters levels.

Proposal 7

We will complete the evaluation of the current Cyber Security Critical National Infrastructure Apprenticeship scheme to inform how to best support the particular critical national infrastructure need in future. We will ensure industry are closely engaged in the evaluation process.

Studying for a university degree is a traditional route of entry into professional life. The NCSC delivers the CyberFirst Bursary Scheme which aims to support and prepare undergraduates for a career in cyber security. The NCSC partners with other government departments and selected industry to offer students £4,000 per year and paid cyber skills training to help them kick start a career in cyber security, either in government or industry. The scheme has supported over 500 bursaries since it was established and has a target of supporting 1,000 students by 2021.

More broadly, the NCSC has certified a number of degree programmes to signpost high quality degrees for those who are interested in pursuing a career in cyber security. Currently the NCSC has certified 23 postgraduate Master's degrees, three Integrated Master's degrees and three Bachelor's degrees. NCSC-certified degrees are key to enabling universities to attract high quality students from around the world, as well as enabling prospective students to make better informed choices when looking for a highly valued qualification. They also assist employers in recruiting skilled staff and developing the cyber security skills of existing employees.

In addition, we want to explore creating a scheme to recognise Academic Centres of Excellence in Cyber Security Education (ACEs-CSE). We envisage these would build on the existing NCSC-certified degree programme and help to

drive excellence by linking together a number of initiatives around outreach, diversity and cyber security education for all university students. We believe ACEs-CSE would help further develop a strong UK cyber security education community and provide a scalable approach for outreach, engagement and teaching of cyber security across universities and communities.

Proposal 8

We will explore options for setting up Academic Centres of Excellence in Cyber Security Education across the UK.

To make the most of the highest levels of academia, in 2013 we established two dedicated Centres for Doctoral Training in Cyber Security Research which have supported 20-30 students a year to undertake a four year doctoral programme, including a taught first year in cyber security. The Centres foster an interdisciplinary environment, welcoming students from a wide range of academic disciplines. Students gain a grounding in core cyber security knowledge and tackle collaborative projects with industry, as well as building doctoral level research skills. Graduates from the early intakes have gone on to roles in academia, government, tech firms and start-ups.

Proposal 9

We will continue to support the next generation of Centres for Doctoral Training that include a cyber security focus. Government will also continue to work with universities across the UK to directly support doctoral study in areas of strategic interest related to cyber security.

Further and higher education are traditional gateways to employment and will remain a fundamental route to entry. However, it is important that relevant courses stay abreast of technological

developments and cyber threats and are teaching students the fundamentals and principles of cyber security, as well as the transferable skills that can be developed further in a professional environment.

It is important to acknowledge that not all cyber security roles are technical in nature. We must therefore ensure that proper consideration is given as to how we can capture those with the aptitude and skills that can be applied to other cyber security roles that are in high demand. In Scotland, for example, the University of Highlands Islands will soon begin delivery of a Masters-level module in 'Managing Cyber Risk' aimed at senior managers in organisations who have a remit for resilience and essential services. While the work being done to demystify cyber security careers - setting out the different roles within the sector and mapping career pathways to achieving them - will promote these different options, there is more we can do to directly tap in to this talent pool.

Proposal 10

We will explore how government and industry can attract new and untapped talent to careers in cyber security, to boost numbers and diversity of those entering the workforce.

This will include how to support individuals with the aptitude and skills for non-technical cyber security roles, such as cyber security policy or strategy positions, and how to better capture and support new and recent graduates in pursuing a career in cyber security, for both technical and non-technical roles. For example we will explore increased provision of placements and incentives for cyber security graduate schemes.

FOCUS ON: Diverting individuals at risk of breaking the law

The UK Serious and Organised Crime Strategy⁴⁰, published in November 2018, recognises the need to divert individuals from re-offending or getting involved in cyber crime in the first place. The limited evidence suggests that those at risk of offending regularly lack an understanding of the legal and ethical issues that present themselves when using certain skills associated with cyber security.

At the same time, the advanced skills that some of the Prevent target audiences possess are in high demand, and if diverted to more meaningful activity before engaging in crime their skills could present an opportunity for a more positive future. An effective response against the threat from cyber crime requires a joined up approach with the UK's Cyber Crime Prevent strategy led by the Home Office.

Proposal 11

Using the convening power of government, and developing a stronger connection between law agencies and the range of CyberFirst programmes, cyber security employers will link up with law enforcement agencies to explore what interventions they both may be able to offer those people identified as at risk.

Extra curricular activities

While formal education plays a significant role in providing young people with the building blocks of digital skills that they need to build a career in cyber security, the importance of activities outside of the classroom in inspiring and promoting cyber security as a profession cannot be underestimated. It is particularly important for those who do not naturally thrive in a formal education environment. During the first two years of the NCSP, we have developed and delivered a number of interventions designed to identify and harness future talent, paying particular attention to the diversity of the talent pool.

Our flagship £20 million Cyber Discovery programme is aimed at 14-18 year olds and brings together real-world cyber expertise and educational experience to find and nurture the next generation of cyber security technical leaders. Over 23,000 students have registered for Cyber Discovery since it launched in late 2017, of which more than 50% completed six or more of the online challenges, with 170 high achieving students winning a place at an industry-led bootcamp. Now in its second year, we expect to see many more young people engage and reach high levels of technical competence, as well as a genuine interest in pursuing a cyber security career.

FOCUS ON: Cyber Discovery - tapping into the cyber security leaders of tomorrow

The government launched Cyber Discovery in 2017, with the aim of supporting the UK's cyber security skills capability by identifying and engaging young people and nurturing their interest in cyber security as a future career path.

The programme is an important component of CyberFirst, the government's cyber security education and skills programme, and is designed to ensure that many more people enter the cyber security profession in the coming years.

Delivered for the government by SANS Institute, Cyber Discovery is a free, extra-curricular programme that is open to young people aged 14-18 years old across the UK. The programme takes participants through a comprehensive, online, cyber security curriculum which uses gamified learning created by cyber security industry experts. It covers everything from digital forensics, defending against web attacks and cryptography, to Linux, programming and ethics, and seeks to provide a clear entry path to future cyber security roles. The course content is fun and challenging, delivered through a role-playing game and mixing online teaching, with face-to-face learning opportunities and real-world technical challenges.

The programme is designed to challenge students through progressively harder material. Students who qualify through the first digital phase - Assess - are then invited to continue to two further online phases - Game and Essentials - where they take on the role of a security agent; gathering information, cracking codes, finding security flaws and dissecting a cyber criminal's digital trail using in-tool resources and research techniques.

Students are supported by online tutorials and by mentor-led after school clubs, often run by computer science teachers, as they find that the curriculum and resources support and extend the current GCSE computer science content.

The top performing students are invited to the final, face-to-face phase of the Challenge - CyberStart Elite Bootcamps. Here they work together in teams, taking on complex, real-world technical challenges, meet industry leaders to find out what it is like to work in the sector, and receive practical help in how they can progress to further cyber security study or jobs.

The first year of the programme has already identified highly talented students who have the skills to become the cyber security professionals of the future:

- Over 23,000 played CyberStart Assess, with 12,500 achieving high enough scores to go through to the main part of the programme CyberStart Game and Essential
- Over 800 students reached the highest level Cyber Start Elite and 170 students were selected to attend two-day bootcamps in the summer of 2018
- 60% of students who, having played Game, would now consider a career in cyber security
- 75% of students who played in year 1 considered returning to Cyber Discovery in year 2
- 91% of club leaders said they would like to carry on with Cyber Discovery in year 2

"One of the problems that I always found looking at the cyber security industry from the outside was the lack of any entry-level programmes. Looking forward in the short term, I am extremely excited about the CyberStart Elite Camps ('hack the robot arm' and Capture The Flag competitions), but in the long term, I'm actually most excited for the doors that Cyber Discovery has opened for me."

Daniel, 17 year old Cyber Discovery Student

The CyberFirst Girls' Competition is another example of an extra-curricular activity that is specifically aimed at inspiring girls to consider studying a GCSE in computer science and pursue a career in cyber security. The 2018 competition saw 4,500 young women from 400 schools participate. In 2019, we will extend the competition to include a week long event to encourage competitors to continue to pursue cyber security as an interest, and as a potential future career. It is not just government that is investing in this area. Wider industry also recognises the impact that providing extra-curricular events and challenges can have on capturing the imagination of those less engaged, or not in formal education. There are many excellent industry and wider cyber security community led extra-curricular activities on offer. For example University Technical Colleges run cyber security curricula for 14-18 year olds, working directly with cyber security employers, and the Cyber Security Challenge UK has worked with industry partners to design challenges and run a series of competitions aimed at testing cyber security skills from those beginning secondary school to those seeking a career change.

While these interventions are capturing and fostering the talent of many cyber security specialists, we acknowledge that they are presently disproportionately focused on developing the more technical cyber security skills. However, we know that addressing the capability gap requires a much broader range of skills and more must be done to account for those other aptitudes and skills that are directly relevant to cyber security.

Proposal 12

We will continue to invest in extra-curricular activities, such as Cyber Discovery and the relevant aspects of CyberFirst, to inspire young people of school age across the UK to understand and consider a career in cyber security. This will include exploring additional extra-curricular activity to develop non-technical cyber security skills for 14-18 year olds.

Proposal 13

We will explore an extra-curricular cyber security learning platform for young people aged 5-14.

.....

CASE STUDY: Wider impact of the CyberFirst Girls' Competition

Kye Academy in Ayr has used the opportunity of the CyberFirst Girls' Competition to achieve a gender balance in its delivery of Scotland's national cyber security qualifications. Scott Hunter, a teacher at the school, entered several teams in the 2017/18 round of the Competition and the experience so inspired girls at the school that 13 girls are now studying for a National Progression Award in Cyber Security at the school, with one class split 50-50 boys and girls.

Mr Hunter says, "We've had great success in inspiring boys to take the qualification in the past, but the Girls' Competition has really helped us show girls that they too can learn cyber security skills and work towards a well-paid and rewarding career".

.....

FOCUS ON: A more coherent offering

There has been significant progress to increase the number of entry points into a career in cyber security, but we recognise that the range of government and industry led initiatives can sometimes be confusing and overwhelming, or hard to find.

We need to bring greater coherence and coordination to the range of initiatives that are offered in a way that is consistent and accessible. There is a range of activity underway to address this, however we recognise that we need to do more. We recently completed a review of the CyberFirst brand to enable us to unify all existing and potential initiatives under one single brand and ensure that the new brand appeals to all ages and experience. This will help to simplify the offering to the public and industry partners, promoting and driving up participation.

It will also help government and industry work more effectively together. CyberFirst, in its current form, is supported by over 50 companies and 19 government departments. By bringing more government cyber security skills activity under the CyberFirst brand, we believe industry will be able to take a much more informed view of where to target their support and efforts. We also want to encourage industry to take on and deliver CyberFirst content to give it a much broader reach.

Proposal 14

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.

Proposal 15

We will continue to encourage industry to use CyberFirst content to deliver additional events and further boost the provision of extra-curricular initiatives.

FOCUS ON: Diversifying the workforce

Ensuring the UK has the capability, diversity and professionalism within the cyber security workforce to meet our needs across all parts of the economy is a critical part of the Develop strand of the NCSS and has been a dominant theme throughout this initial strategy.

We need a sector in the UK that has the diversity of background and life experience that brings different insights, creates challenge and encourages change and innovation. A diverse workforce, with a mixture of both technical and non-technical skills, is essential for the sustainability of the UK's cyber security sector, ensuring the UK is the best place to be a cyber security professional, and ensuring the UK is the world's leading digital economy.

While the numbers vary according to different research methodologies and areas of focus, there is little dispute that the gender split within the UK tech sector is not reflective of the wider population. At a global level, research suggests women comprise only 11% of the global cyber security workforce.⁴¹

This is simply not good enough. The government is committed to addressing this problem and has invested in and committed to a range of programmes that seek to redress that imbalance, complementing a range of non-government programmes designed to encourage women into tech and cyber security.

For example, the CyberFirst Girls Competition is designed to give as many girls as possible the opportunity to find out more about cyber security with a view to potentially influencing the subjects they take as qualifications. The CSIIIF includes projects that help female returners to work who have been out of the labour market due to caring responsibilities. We will continue with this approach to stimulate the market to develop initiatives that specifically target women.

More broadly the Tech Talent Charter encourages and supports signatories to tackle the issues around female under-representation in the tech sector by undertaking to support attraction, recruitment and retention practices that are designed to increase the diversity of their workforce.

We are not alone in recognising the urgent need to address the issues surrounding gender in tech, and cyber more specifically. There are a range of private sector programmes that each have a unique take on how to make positive change, including Women in Tech (techUK)⁴², EMEA Women in Cyber (Deloitte)⁴³, Tech She Can Charter (PwC)⁴⁴, SheLeadsTech (ISACA)⁴⁵ and Code First Girls.⁴⁶

However, it is not just about ensuring a more representative gender balance in the cyber security profession. In the UK there are around 700,000 people on the autism spectrum.⁴⁷ Less than a fifth (16%) of adults with autism are in full time employment, and a third (32%) are in any form of paid work at all.⁴⁸ These individuals present a well of untapped potential, as it is estimated that more than three-quarters of cognitively able adults with autism have the aptitudes and interests that make them suitable for careers in cyber security. These skills include analytical thinking, focus and attention to detail.⁴⁹

We are also actively working with the private sector, academia and the third sector to ensure that opportunities in the sector are accessible to neurodiverse individuals. The Cyber Neurodiversity Group has over 30 members representing the UK Government, the UK cyber industry, academia and the third sector. The Group aims to use its shared knowledge and experience to attract and retain those with neurodiverse conditions into the cyber security sector.⁵⁰ These activities range from specific career and industry events, such as NeuroCyber:2 for neurodiverse individuals through to cross sector working groups.

We will continue to invest in initiatives that seek to redress this imbalance and will evaluate their impact to determine future approaches.

Call for views

This chapter sets out the steps we will take to attract diverse talent into the profession by supporting opportunities to inspire the current workforce to retrain as cyber security professionals, as well as putting in place the building blocks for future careers in cyber security through formal educational and extra-curricular activities that will inspire future cyber security professionals. A key component of this is providing greater coherence and coordination to the range of initiatives that are offered.

- What more can government and industry do jointly to make more cyber security retraining opportunities available to a broader and diverse range of adults?
 - We have set out a proposal to demystify cyber security careers - this will map different career options and pathways to ensure there is clear and accessible advice for anyone who has the aptitude for a career in cyber security. Are there any other specific outputs or products that you would like to see as part of this work?
 - We propose appointing one or more independent Cyber Security Skills Industry Ambassadors to help promote the profile, attractiveness and viability of a career in cyber security to a broader and more diverse range of individuals. We envisage the role will also help distil and represent views of the cyber security community to government and vice versa. Do you agree or disagree with the proposal to appoint Cyber Security Skills Industry Ambassadors?
 - We are aware that more needs to be done to develop and nurture individuals with the aptitude and skills for non-technical cyber security roles. Do you think government should prioritise this?
 - We propose exploring what more can be done to support untapped and more diverse talent, including women, neurodiverse individuals, graduates and others with the aptitude and skills for cyber security roles. How do you think government and industry can creatively work together to quickly achieve a more diverse cyber security workforce?
-

Chapter 6

Broader Cyber Security Capability for a World Leading Digital Economy

Chapter 6 – Broader Cyber Security Capability for a World Leading Digital Economy

Overview

Maintaining the resilience of the digital economy is not the sole responsibility of cyber security professionals. This chapter sets out how we will work towards embedding cyber security across the whole of the economy, including basic cyber security hygiene of employees and citizens, informed cyber security risk management of those who operate businesses or services, and the embedding of cyber security within professional disciplines across every sector.

Objective 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

While the development of the cyber security profession and a vibrant education and training ecosystem is fundamental to meeting the current and future need for specialist cyber security professionals, it is not enough to ensure the security and resilience of the wider digital economy.

As set out in the strategic context, cyber security cannot and should not be the sole responsibility

of cyber security professionals; there must be a broader expectation for everyone in the workforce, across every sector, to have a proportionate understanding of cyber risk management. The level and depth of understanding required will naturally vary according to the nature of the position, however this can be grouped into three main tiers.

First, it is critical to ensure that there is a general foundation of cyber security understanding across the general population and workforce, largely increasing the surface area of defence which will mitigate against the vast number of high-volume, low-sophistication attacks.

Second, we must also ensure and remain confident that those who require cyber security services have the knowledge and understanding they need to be equipped to make the most appropriate choices. This ranges from those who are responsible for securing our critical national infrastructure and other key sectors, to those who run business across all sectors of the economy, from large organisations to small and medium sized enterprises (SMEs).

Third, we must 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.

Embedding basic cyber security universally

Everyone should be digitally literate and have an awareness of cyber risks, including being able to take the most basic steps to mitigate them. This means adopting simple measures such as using

strong and separate passwords for online accounts and updating apps and software as required.

The UK Digital Strategy⁵¹ sets out the government's approach improving digital inclusion, of which basic cyber security awareness is a component. As part of this, the government is introducing an entitlement to full funding for basic digital courses from 2020. Adults will have the opportunity to undertake improved digital courses based on new national standards that the Department for Education (DfE) has published as part of its consultation on plans to improve adult basic digital skills. These standards, based on the Essential Digital Skills Framework⁵² developed by Lloyds Banking Group and the Tech Partnership, will set out the skills and capabilities people need to get on in life and work with a strong focus on being safe and responsible online.

The need for universal digital skills is being recognised within our education system. For example, for post-16 students DfE is introducing new T Levels in England, based on employer-designed standards and content, and backed by £500 million investment a year. Once implemented, T Levels will include a substantial industry placement as part of the programme. All T Levels are designed to develop the digital skills required to succeed in the modern workplace, and the Digital (Digital Production, Design and Development) T Level is one of the first three T Levels to be taught by a small number of providers from September 2020. The roll out of T Levels will be phased with all 25 T Levels available from 2023. In Scotland, Digital Literacy forms part of the 3-18 curriculum, with cyber resilience sitting alongside internet safety within its learning outcomes.

Employers are also designing new apprenticeships that are more responsive to the needs of business and we have supported many to develop new apprenticeships in digital occupations across different levels, up to degree level, including in data analysis, digital marketing, network engineering and cyber security. The Institute for Apprenticeships is

required by law to review apprenticeship standards regularly and announced on 20 September 2018 that 12 digital apprenticeships, including two cyber standards, will be the first to be reviewed. The employer consultation concluded in October 2018⁵³ and outcomes will be published early in 2019.

We will also continue to support the creation of new courses, facilities and ways of learning through the Institute of Coding (IoC). IoC will improve our high level digital skills capability, including cyber security, through a wide consortium of universities, professional organisations and employers which will improve the flow of graduates into the labour market with the degree level digital skills needed by tech recruiters - including cyber security. A number of new courses started in September 2018 and will be evaluated as part of the IoC's remit.

Similarly, Ada National College for Digital Skills (Ada) specialises in higher level training for digital specialisms and over the next 10 years aims to expand its reach across the UK and train up to 10,000 learners in a wide range of digital careers. Ada has already developed content to support cyber security specialist higher apprenticeships and is ready to deliver these as and when the industry requires.

Through the Digital Skills Partnership (DSP), launched in July 2017, we are working to bring together organisations across all sectors to tackle the digital divide. A key priority is to support the formation of Local DSPs in Local Enterprise Partnership regions, which will design, develop and deliver innovative digital skills programmes to advance digital inclusion and upskill the current workforce. National level Delivery Groups will support the local work and other sub groups such as the Computing in Schools Delivery Group which bring together industry and non-profit organisations to support the teaching of computing in schools. In Scotland, the Scottish Government is working with the non-formal learning sector to provide guidance for workers and adult learning tutors on how to build cyber security resilience into digital literacy.

Proposal 16

Government will continue to support these initiatives and explore how they can expand, as required, to keep pace with changing technology and the changing digital needs of the workforce.

Embedding cyber security within professional decision making

Increasing the capability and understanding of those who require cyber security skills will enable them to be more informed about the professional services they require, and equip them to manage their recruitment or outsourcing in a way that actually meets their needs. Not only will this have a direct impact on any cyber skills shortage, by helping to focus the scope of the services required, but it will ensure that cyber security risk is being appropriately managed.

Small business owners, as well as boards of larger organisations, for example, need to understand the impact that cyber attacks can have on their businesses and be able to manage them in a proportionate way. To do that effectively requires a level of awareness and understanding about those risks and what mitigations need to be put in place to manage them. Having this understanding will equip boards and business owners to recruit the right staff or take control of any outsourced cyber security services.

While consciousness of cyber security as a risk is growing, wide-spread capability gaps are evident. For example 47%⁵⁴ of boards of FTSE 350 companies do not have a clear understanding of the potential impacts resulting from a loss of, or disruption to, key information or data assets, and only 27% of businesses and 21% of charities have a formal cyber security policy or policies.⁵⁵

The government is progressing a wealth of activity

focused on ensuring that UK organisations are able to effectively manage their cyber risks, from the issuing of consistent and targeted advice and guidance to putting in place the necessary incentives.

The NCSC, as the technical authority for cyber security, provides a plethora of simple and targeted guidance and tools aimed at providing the necessary knowledge to equip all types of organisations to be able manage their cyber risks. This includes the 'Small Business Guide'⁵⁶, which supports SMEs in improving their cyber security quickly, easily and affordably, and the development of a toolkit to support boards to better understand and prepare for managing cyber threats.

The NCSC also operate 'Cyber Essentials',⁵⁷ a government-backed certification scheme which focuses on key technical controls that all organisations, including SMEs, charities and the public sector, should have in place to help protect themselves against the most common forms of online threats. This scheme is currently being strengthened to ensure that it is having the greatest impact. The NCSC also publish the '10 Steps to Cyber Security' which outlines further key measures for high tech SMEs and larger scale public and private organisations. The NCSC will continue to engage with UK organisations to ensure they have the knowledge they need to effectively and proportionately manage their cyber risk.

DCMS is also considering how the government can further equip organisations to make informed decisions regarding their risk profile, including consideration of how best to incentivise more proactive cyber risk management across the economy. Having an informed approach to risk management should enable an organisation to identify the cyber security capability it requires.

Proposal 17

DCMS will continue to explore how to further equip and incentivise organisations to better understand their cyber security risk profile and take informed action in response.

Embedding cyber security within professional disciplines

As the digital economy grows, the need for adequate cyber security to protect the integrity, confidentiality and availability of the data flows on which it depends, becomes increasingly acute. Some sectors of the economy in particular, such as the financial and legal sectors, will need to take particular care.

Given the inherent nature of cyber threats to a digital economy, cyber security must become embedded by default - 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 need to become integrated into the very 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. We acknowledge, however, that the Council will take some time to establish itself and there is a more pressing need to explore with other professions and disciplines how we can embed cyber security within professional codes of conduct or codes of ethics.

The Scottish Government is committed to exploring a revision of National Occupational Standards (NOS) for cyber security, building on existing

NOS for Information Security. It will do this in collaboration with the Welsh Assembly and the Government of Northern Ireland, with consultations taking place with industry across the whole of the UK. These NOS will be used to assist employers in designing jobs but also in the creation of fit-for-purpose qualifications.

Only by embedding cyber security in this way will we affect a culture shift within whole professions across the economy that will ingrain the cyber security understanding that is demanded to maintain the security and resilience of the digital economy.

Proposal 18

We will work with other professions to embed cyber security within relevant professional codes of conduct / codes of ethics ahead of the UK Cyber Security Council taking the leadership.

We must also strive to ensure that cyber security is considered implicitly in the development of emerging technology and future related strategies. For example, while the adoption of AI in industry will provide great benefits in terms of productivity, it will also present vulnerabilities given the increasing connectivity of such systems. To not give cyber security adequate consideration during the development and adoption would undermine AI's integrity and place the wider economy at risk.

This is true of all of emerging technology that provides the means of transferring data across the digital economy.

Proposal 19

We will work across government and wider industry to ensure that cyber security is adequately reflected in the implementation of emerging technologies and associated strategies.

Call for views

This chapter sets out how we will work towards embedding cyber security across the whole of the economy, including basic cyber security hygiene of employees and citizens, informed cyber security risk management of those who operate businesses or services, and the embedding of cyber security within professional disciplines across every sector. We have had some early successes but recognise much more needs to be done.

- Are there any specific initiatives that you think government and industry should focus on in order to increase the cyber security capability across the general workforce?
 - We propose working with other professions and disciplines to embed cyber security in codes of conduct and codes of ethics and to ensure cyber security is adequately reflected in the implementation of new technologies. Which of the following sectors should the government prioritise?
 - Construction
 - Education (including academies)
 - Entertainment
 - Finance or insurance
 - Food or hospitality
 - Health, social care or social work (including NHS)
 - Information or communications
 - Legal
 - Other public sector
 - Retail or wholesale
 - Scientific or technical
 - Technology sector (including emerging technologies)
 - Transport
 - Utilities or production (including manufacturing)
 - Other
-

Chapter 7

Leading the Way

Chapter 7 – Leading the Way

Overview

Cyber Security is a global sector in which the UK plays a leading role. We have strong international partnerships, cyber security professionals who are respected and trusted around the world and an approach to developing new talent which is considered creative and innovative by our allies. This chapter sets out the UK's approach to maintaining the best talent and how the public sector, across all parts of the UK, can lead by example in addressing the cyber security capability while being open to creativity.

Objective 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

Having a sustainable supply of home-grown cyber security professionals is part of our wider ambition to be a world leader in cyber security. Put simply, we cannot be a global leader in cyber security without access to the best cyber security talent.

This is about both attracting new and untapped talent into the profession and ensuring the UK is the best place in the world to be a cyber security professional, so that we retain new talent and attract the best from the rest of the world. Having that talent in the UK is central to making the UK the world's leading digital economy and provides important international trade opportunities.

We believe, with the range of work set out in this initial strategy, that the conditions exist for that

to happen. We equally believe the public sector should, where appropriate, set the example - to demonstrate the benefits of comprehensive cyber security to both individual organisations as well as the wider UK economy.

The public sector leading by example

The government, devolved administrations and the wider public sector hold large quantities of sensitive data, deliver essential services to the public and operate networks that are critical to our national security and resilience. While we continue with the modernisation of our public sector services, outlined in our Digital Strategy, we recognise more needs to be done. In order to counter the risks posed by our adversaries, whether professional hackers, organised crime syndicates or nation states, we need a skilled cadre of cyber security specialists and the right broader cyber security capability.

This is why we are placing a major focus on upskilling the public sector workforce, from board level to administrative assistants, in order to keep our systems and data safe. Every part of the public sector needs a workforce plan to address its cyber security capability gap. These plans should include a strong focus on apprenticeships, retraining and retention of talent.

We want the UK public sector to be an exemplar for the wider economy on cyber security capability. This section outlines some excellent examples of where government is already leading in developing cyber security capability, such as in the NHS and in Policing. But we recognise we need to do, and be seen to be doing, more. By investing further in our people, alongside our systems, and showcasing our successes, we want to show the rest of the economy that cyber security and a cyber secure workforce is one of our highest priorities, and should be theirs too.

Proposal 20

We will continue to invest in the cyber security capability of the public sector to ensure that infrastructure, services and assets are protected, and to set the example to other sectors across the economy.

CASE STUDY: A review of government security

A review of government security in 2016 ('Transforming Government Security: Review' March 2016) highlighted weaknesses in existing security systems that posed a significant and increasing risk to the way government is able to carry out day to day business. The review assessed that government security had broadly been carried out in the same way for over 30 years. This is not viable and far-reaching, as fundamental changes are needed to improve our security to equip us to deal with 21st century demands and challenges.

To address this, the Transforming Government Security Programme (TGSP) was set up in 2017 and set out to establish a government wide Security Profession (GSP) that would ensure that staff had the appropriate skills and training needed to provide world class security services for government. The ambition for the GSP is to provide clear career pathways to higher positions for subject matter experts, such as those in cyber security, to enable government to deliver services securely.

As a way to attract talent into the workforce immediately, the GSP has adopted a recruitment scheme for apprentices for central government. The majority of recruits are young students that are still studying (between 18 to 19 years old) and 10-15% are in their 30s or 40s looking for a career change. Students have generally obtained their A levels, but this is not a requirement. In most cases, students are recruited into government upon completion of the apprenticeship. Since the beginning of the scheme in 2015, the profession has taken in approximately 25 apprentices each year. The scheme is intended to increase the number of recruits and become the main point of entry for cyber security professionals in government.

The GSP also make efforts to attract candidates from a variety of backgrounds, including neurodiverse individuals. The skills the GSP mainly look for are 'office skills', such as strong communication, team working abilities and attention to detail. It is important the candidates demonstrate an interest in cyber security and working for government. The objective of the GSP is to mainstream the recruitment of cyber security entry-level professionals for central government and address the gap of professionals at High Executive Officer (HEO) and Senior Executive Office (SEO) levels who frequently leave after training to work for the private sector.

FOCUS ON: The Scottish Government's commitment to developing cyber skills

In March 2018, the Scottish Government published its Learning and Skills Action Plan, with 37 actions to support the development of cyber resilient behaviours and to help build a skilled and growing cyber security profession for Scotland.

This action plan sets out 4 overarching aims to successfully grow Scotland's cyber resilience learning and skills landscape. These aims are to:

1. Increase people's cyber resilience through awareness raising and engagement
2. Explicitly embed cyber resilience throughout the education and lifelong learning system
3. Increase people's cyber resilience at work
4. Develop the cyber security workforce and profession to ensure that skills supply meets demand and that skilled individuals can find rewarding employment in Scotland

The strategy is closely aligned with the UK National Cyber Security Strategy. Cyber security is a reserved matter, but it has strong implications for the delivery and resilience of devolved services. As such, the Scottish Government works closely with the government and the UK's National Cyber Security Centre (NCSC) to ensure alignment between work on cyber resilience at the UK wide and Scottish levels.

CASE STUDY: Local government

Through the NCSP the Ministry of Housing, Communities and Local Government (MHCLG) has implemented a number of initiatives across local public service and resilience communities, to improve their cyber resilience and upskill seniors leaders.

From January 2019, MHCLG will be rolling out the NCSP National Capabilities "Pathfinder" Training Scheme. This comprises the creation of a local public sector training scheme, cyber exercise programme and, through the ResilienceDirect platform, a cyber hub which will provide a one stop shop for all key cyber related material and guidance. Collectively this will deliver over 3,000 training places and online access to the learning materials and cyber exercising formats for local public service leaders, policy makers and practitioners and partners within local resilience forums in 2019 and 2020. Beyond 2020, The "Pathfinder" Training Scheme and Exercise programme will be supported by a Cyber Academy, to launch during 2019, that will support the ongoing delivery, continuous improvement and roll out of these programmes.

The "Think Cyber Think Resilience" NCSP regional showcase initiative has to date inducted over 2,000 local public sector leaders and practitioners in the wider NCSS. The linked Cyber Hub programme will ensure that local authorities and their partner forums can access NCSP developed services and solutions.

The result of these schemes will be the embedding of robust cyber resilience arrangements across mayoral/combined authorities and multi-agency partnerships.





CASE STUDY: The armed forces

The Ministry of Defence (MOD) has a greater need than most organisations for innovating in cyber security. A successful cyber attack against the UK can put critical national infrastructure, vital communications, defence forces and even the lives of UK citizens at risk. Given its role in safeguarding the UK, the MOD is investing in cyber security innovation to increase national resilience to cyber attacks through both defensive and offensive measures. The MOD is also collaborating with industry to combat the growing cyber threat. To be at the forefront of cyber security, the MOD needs to recruit and maintain a specialist cyber workforce.

To identify cyber security talent within its existing workforce, the MOD has developed the Defence Cyber Aptitude Test (DCAT). DCAT enhances the military's existing selection measures for personnel already serving who hope to get posted to a cyber unit in the future. The test itself comprises a number of sections and tests an individual's abilities across a range of cognitive challenges - prior technical knowledge is not measured. The DCAT is being rolled out across UK defence for use at the early stages of technical training and service careers.

In March 2018, the initial phase of the new Defence Cyber School was opened. The school will address specialist skills and wider education in the armed forces. The school is located at the Defence Academy site in Shrivenham which facilitates its close involvement with the Cranfield University, the academic provider for the Defence Cyber Masters Programme. Work continues to significantly increase both the teaching capacity and the range of courses available at the DCS.

The MOD has also delivered an annual Inter-Services Cyber Network Defence Challenge over recent years. The 2017 Challenge was organised by Joint Forces Command and pitted four teams from the Army, Royal Navy, Royal Air Force and Civil Service. The competition involves challenges that test both individual technical ability and team working of experienced cyber professionals - the 'capture the flag' based event is designed to test and teach those who attend to counter cyber attacks. Teams are supported by industry cyber instructors to ensure that learning is maximised throughout the competition.



CASE STUDY: The NHS in England

Health and Care is a uniquely federated system with 1.4 million employees in health and at least 1.5 million involved in care provision. In order to deliver the outcomes required by an ageing population and greater demands on the system, there is a requirement to digitise rapidly. Due to the scale of workforce and range of digital maturity, there is a need to provide different levels of training to ensure good cyber security practice is embedded within every digital transaction.

NHS Digital's Data Security Centre, working as part of the Department of Health and Social Care's Cyber Security Programme, has delivered tiered e-learning packages that cater from general employee level up to board level for individual organisations. This recognises that good cyber security practice is a workforce wide responsibility, driven across all areas of an organisation.

In terms of specialist skills, health and care struggles with the same challenges faced across the public sector. There is a high demand for cyber security professionals and there are private organisations that are able to offer much greater remuneration to try and attract the best talent. To mitigate this, NHS Digital is partnering with major industry sector leaders to bolster capability, whilst also training an increasingly diverse new workforce with graduate, apprenticeship, and the newly created 'Women in Cyber' schemes. Training is offered to all cyber security professionals as a method of retention, together with the unique nature of the role defending health and care and the job satisfaction this can bring.

CASE STUDY: Boosting cyber capability in law enforcement

For successful investigations and prosecutions, law enforcement needs to have capable cyber security professionals with a particular blend of skills. This is particularly challenging because the retention of law enforcement officers and staff in specialist cyber investigation roles remains an acute problem. Law enforcement agencies surveying of future candidates have confirmed that the professionalisation of cyber investigation is a significant factor in improving retention and recruitment.

To address this, the College of Policing is working on behalf of the Home Office on a Cyber Digital Career Pathways (CDCP) project. This project will create a Cyber Digital Investigation profession within Law Enforcement, supported by a dedicated Institute and accredited national training register. It will provide a career pathway and professional certification for Cyber Digital Investigation Professionals who are defined as 'A person at the core of cyber digital investigations, who may have to present evidence at court of their cyber digital investigation skills'.

This will complement and align with the broader proposals to develop the cyber security profession which is covered in detail in chapter 4. The Career Pathway will create 'multi agency' standards within which Cyber/Digital Investigation Professionals are recruited, retained and developed. This will enable interoperability between police forces, wider law enforcement and partners, with the ultimate goal of setting the industry standard 'profession' of Cyber Digital Investigation/Security Professional.

Engaging globally

The UK is truly a global leader in cyber security. We have a thriving and vibrant cyber security sector. There are an estimated 846 UK firms providing cyber security products and services, earning the economy a total revenue of £5.7 billion in 2015.⁵⁸ The majority of these businesses are Micro and SMEs (89%), and account for 26% of revenues.⁵⁹ Between 2015 and 2017, over 100 new businesses were registered within the cyber security sector and in this period the number of micro firms doubled.

We have long-standing defence and security relationships on cyber security, including those with the United States of America, Australia, Canada and New Zealand, Europe and NATO. In June 2014, the UK became a full member of the NATO Cooperative Cyber Defence Centre of Excellence in Estonia, which exists to enhance capability, cooperation and information sharing in cyber defence. Furthermore, in April 2018, the UK hosted the Commonwealth Heads of Government Meeting at which all 53 Commonwealth member states agreed the Commonwealth Cyber Declaration. It is the world's largest inter-governmental commitment to cyber security cooperation and an important expression of our desire to maintain a free, open, inclusive and secure cyberspace.

Given the opportunities and threats presented through cyberspace extend across national boundaries, and cyber security will continue to be a global issue, it is essential that we work with other nations and multilateral institutions so that we are able to operate effectively in a wide range of defence and security situations. Maintaining our position as a global leader in cyber security is particularly critical for attracting and retaining the best home-grown and international talent - it will also lead to continued investment in the UK. Government, industry, academia and the third sector all have a key role to play here.

This is why we are leading and participating in a range of international programmes and initiatives on cyber security that aim to strengthen our global reputation, share best practice with our allies and create a stronger and more cyber secure world. Since the launch of the NCSS and NCSP we have made it a priority to engage with our allies and showcase the best of the UK. This has been done through our academic excellence, international student exchange programmes, international cyber security challenges and playing a key role in conversations with our closest allies, amongst many other initiatives.

UK universities are at the forefront of cyber security research, conducting world leading research projects. For example, the NCSC and the Engineering and Physical Sciences Research Council (EPSRC) have jointly recognised 17 Academic Centres of Excellence in Cyber Security Research. These Centres of Excellence form the backbone of the UK's world leading cyber security research and will help develop the tools to secure technologies for consumers, business and government.

In October 2018, the UK hosted the European Cyber Security Challenge (ECSC). The competition saw 18 countries from across Europe send a team of under 25s to participate in a 'capture the flag' style competition. The ECSC is promoted by the European Commission and promotes friendly relations between attending countries, officials and players.

The first US/UK Future Cybersecurity Leaders Exchange collaboration for 16 and 17 year olds took part in August 2018. The programme included a 10 day exchange in the US for eight British and eight US students and aimed to provide a hands-on introduction to a range of cybersecurity challenges. The UK and US are both very supportive of this exchange and the UK will be hosting the next exchange which is due to take place in July/August 2019.

More broadly, to build cyber security capacity across the Commonwealth, the UK has made up to £15 million available to support implementation of the Commonwealth Cyber Declaration through to 2020. More than £5 million of that will be specifically dedicated to the Foreign and Commonwealth Office's (FCO) Commonwealth Cyber Security Programme, supporting low and middle income countries. The remaining £10m will be delivered through the Prosperity Fund and the international strand of the National Cyber Security Programme. These programmes will promote security and prosperity in the Commonwealth, by providing technical assistance, training and advice to address a wide range of cyber security and cyber crime threats.

By engaging globally, developing people to people links through friendly competition, academia and exchanges, and playing proactive roles in international cyber security conversations we are securing the nation's future as a world leader in this field. We will continue to promote our brightest and our best on the international stage beyond the end of the NCSP, and continue to showcase the highly skilled talent that the UK has to offer.

Proposal 21

We will continue to engage internationally to share and learn from best practice and attract and retain the best home-grown and international talent to the UK.

Call for views

This chapter sets out the UK's approach to maintaining the best talent and how the public sector, across all parts of the UK, can lead by example in addressing the cyber security capability. We acknowledge that there is much more that the public sector can do to achieve this, and we want to understand what the public sector should prioritise to set the most useful examples to industry.

- Are there any specific commitments you feel the public sector in the UK should lead on and adopt in order to set an example for the rest of the UK economy?
- Are you aware of any examples where the UK Government effectively engaged with industry to disseminate information and distil best practice?
- Are you aware of any initiatives or programmes internationally to build cyber security capability that you think would be beneficial if applied in the UK?

Chapter 8

Delivering in Partnership

Chapter 8 – Delivering in Partnership

Overview

Many of the successes delivered so far through the five year National Cyber Security Programme have been informed and shaped by the collaboration between industry and government. This chapter sets out that continued collaboration between all parts of the UK cyber security community is key to delivering the bold and ambitious programme set out here to develop the UK's cyber security capability.

This initial strategy builds on the strong record of delivery over the first half of the five year NCSS and sets out an ambitious programme of additional activity to match our mission to increase cyber security capability. Delivering it will require a whole UK cyber security community approach.

Government will continue to play a key role and use the range of unique levers we have. But to deliver at the level of ambition set out in this initial strategy, we need to build on the collaboration between government and the cyber security community that has been at the heart of many of the successes so far. This reflects that the benefits of the effort to increase cyber security skills will be felt across the public and private sectors.

Much of the investment now is about building the foundations for a programme of work that is sustainable in the long term. For example, government is helping to create the environment for the development of the profession by kick-starting the formation of a new, independent UK Cyber Security Council. The work to define a body

of knowledge for cyber security will also service the profession well over coming years. Both of those areas of work have been shaped by close engagement with the cyber security community and will be owned and led by the community. Beyond that, we want to continue to expand industry involvement in government initiatives. As noted above, we want to bring more coherence to the CyberFirst brand to allow more industry partners to take a more informed view of where to target their support and efforts.

Government also wants to intervene sensibly, where we can help the creativity, innovation and expertise evident in the community to flourish. The public sector needs to both be an exemplar of best practice while being open to creative and innovative ideas and initiatives developed elsewhere. Government backing can help new and exciting initiatives stand-up and scale-up - as we have through the CSIIIF which is designed to boost the cyber security training ecosystem with small amounts of government funding.

The NCSP, underpinning the NCSS, brings £1.9bn of investment over the five year programme. This is a significant investment. The NCSP comes to an end in 2021 and while government will continue to support and drive the long term delivery of the overarching strategic outcome, we must work with the cyber security community to ensure the range of initiatives are sustainable. This includes additional or alternative funding streams. This will be a key part of the conversation between government and the wider cyber security community up until 2021. It is not about unrealistic expectations of altruism but rather ensuring there is a level of support and investment from all parts of the cyber security ecosystem that is commensurate to the benefit obtained from the activity.

Chapter 9

Implementation and Measuring Impact

Chapter 9 – Implementation and Measuring Impact

It is imperative that we fully evaluate the programmes and initiatives that have been developed and delivered during the NCSP. While some interventions, such as those designed to inspire young people into the cyber security profession, will by their nature have a longer lead time, we will conduct interim evaluations wherever appropriate.

Continually building a deeper understanding of which interventions have the most significant impact will enable us to tailor future programmes with the aim of empowering and supporting wider industry to deliver these independently as the market requires.

This initial strategy provides an opportunity for our partners and stakeholders to add to this evidence base and to steer the future direction of policy and intervention where required. We will set out

proposals in the final strategy to ensure that a comprehensive evaluation framework is in place, once our evidence base is more mature.

We will use the call for views, including the engagement process, to develop clear and stretching key performance indicators to ensure that for the remainder of NCSP and beyond we are able to measure the success of our approach.

Because of the nature of what we are trying to achieve, and given the considerable lead in times of many of our initiatives, it is right that we spend time now to define informed performance measures that will ensure we can effectively monitor success over the longer term.

In the meantime, we have defined clear delivery milestones which set out tangible steps to implementing and delivering this strategy.

Objective 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

Delivery milestones	<ul style="list-style-type: none"> ● Delivery partner identified for UK Cyber Security Council ● A clear business plan and roadmap for delivery of prioritised deliverables ● All CyBOK knowledge areas published ● Delivery of initial priorities by Council 	<p>Q2 2019</p> <p>Q4 2019</p> <p>Q4 2019</p> <p>Q1 2020</p>
---------------------	---	---

Objective 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

Delivery milestones	<ul style="list-style-type: none">• Publish evaluation of the current Cyber Security Critical National Infrastructure Apprenticeship, Cyber Skills Immediate Impact Fund Pilot and Cyber Security Postgraduate Bursaries scheme• Cyber Security Skills Ambassador(s) appointed• Launch expanded CyberFirst brand	Q2 2019 Q2 2019 Q4 2019
---------------------	--	-------------------------------

Objective 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

Delivery milestones	<ul style="list-style-type: none">• UK Cyber Security Council to agree approach to embedding cyber security within relevant professional codes of conduct / codes of ethics	Q2 2020
---------------------	---	---------

Objective 4

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

Delivery milestones	<ul style="list-style-type: none">• Government to present and seek feedback from a range of international partners on the strategy	Q1 2019
---------------------	--	---------

Chapter 10

Taking this Forward

Chapter 10 – Taking this Forward

As we have set out, there is huge passion, enthusiasm and expertise within the UK's cyber security community which has been central to the UK becoming a global leader in cyber security. This initial strategy is designed to harness that fully. We have published this as an initial strategy to ensure all of those with an interest in cyber security have the opportunity to engage and help shape and refine the proposals further. Publication starts a ten week call for views.

We have posed a series of questions, set out below and throughout this document, which provide an opportunity to propose further creative and innovative ideas for boosting cyber security skills capability over the remainder of the NCSS and beyond.

We will also run a series of engagement events during early 2019 to explore these questions in more depth - we are keen for as broad a range of representation as possible and there will be events across England and in each of the devolved administrations. Please register your interest by completing the online form.⁶⁰

Following the ten week period of engagement, we will use the evidence received to develop and publish a comprehensive and final strategy document which we intend to publish in 2019. This is your opportunity to help shape the future of the UK's approach to cyber security skills and capability.

Call for views - questions

Please note the questions below are for reference only. Please respond by completing the online survey.⁶¹

Chapter 2 - Strategic context

In this chapter we set out the government's understanding of the challenge on cyber security skills. We believe the challenge is a complex one which represents a cyber skill capability gap in the UK. Yet we know this is felt differently across different sectors and parts of the economy. We want to validate our assessment of the cyber security capability landscape and identify where there may be additional or further challenges in specific parts of the economy.

- To what extent do you agree with government's assessment of the strategic context?
- Do you think there are any other challenges or issues that are not covered in the government's assessment of the strategic context?

Chapter 3 - The national response: our mission

This chapter sets out government's longer term mission on cyber security skills to increase cyber security capability across all sectors. It also defines four proposed objectives to deliver that mission. We want to understand whether or not the level of ambition articulated through the mission and objectives is sufficiently ambitious to meet the challenge.

- To what extent do you agree that the mission and objectives set are sufficiently ambitious to address the challenges identified?
- Why do you agree/disagree that the mission and objectives are sufficiently ambitious?

Chapter 4 - A structured and trusted profession

This chapter sets out the decisive action being taken to develop a clear definition of cyber security skills, an agreed body of knowledge, and to create a new, independent UK Cyber Security Council as the focal point for the cyber security profession in the UK. We have recently consulted on developing the cyber security profession and CyBOK knowledge areas continue to be consulted on. We acknowledge, however, that there are still challenges around taxonomy and defining cyber security skills. We are therefore seeking to understand whether the definition of cyber security skills set out above reflects the consensus view in the UK cyber security community.

- Do you think there is anything missing from the definition of cyber security skills?

Chapter 5 - A vibrant education and training ecosystem

This chapter sets out the steps we will take to attract diverse talent into the profession by supporting opportunities to inspire the current workforce to retrain as cyber security professionals, as well as putting in place the building blocks for future careers in cyber security through formal educational and extra-curricular activities that will inspire future cyber security professionals. A key component of this is providing greater coherence and coordination to the range of initiatives that are offered.

- What more can government and industry do jointly to make more cyber security retraining opportunities available to a broader and diverse range of adults?

- We have set out a proposal to demystify cyber security careers - this will map different career options and pathways to ensure there is clear and accessible advice for anyone who has the aptitude for a career in cyber security. Are there any other specific outputs or products that you would like to see as part of this work?
- We propose appointing one or more independent Cyber Security Skills Industry Ambassadors to help promote the profile, attractiveness and viability of a career in cyber security to a broader and more diverse range of individuals. We envisage the role will also help distil and represent views of the cyber security community to government and vice versa. Do you agree or disagree with the proposal to appoint Cyber Security Skills Industry Ambassadors?
- We are aware that more needs to be done to develop and nurture individuals with the aptitude and skills for non-technical cyber security roles. Do you think government should prioritise this?
- We propose exploring what more can be done to support untapped and more diverse talent, including women, neurodiverse individuals, graduates and others with the aptitude and skills for cyber security roles. How do you think government and industry can creatively work together to quickly achieve a more diverse cyber security workforce?

Chapter 6 - Broader cyber security capability for a world leading digital economy

This chapter sets out how we will work towards embedding cyber security across the whole of the economy, including basic cyber security hygiene of employees and citizens, informed cyber security risk management of those who operate businesses or services, and the embedding of cyber security within professional disciplines across every sector. We have had some early successes but recognise much more needs to be done.

- Are there any specific initiatives that you think government and industry should focus on in order to increase the cyber security capability across the general workforce?
- We propose working with other professions and disciplines to embed cyber security in codes of conduct and codes of ethics and to ensure cyber security is adequately reflected in the implementation of new technologies. Which of the follow sectors should the government prioritise?
 - Construction
 - Education (including academies)
 - Entertainment
 - Finance or insurance
 - Food or hospitality
 - Health, social care or social work (including NHS)
 - Information or communications
 - Legal
 - Other public sector
 - Retail or wholesale
 - Scientific or technical
 - Technology sector (including emerging technologies)
 - Transport
 - Utilities or production (including manufacturing)
 - Other

Chapter 7 - Leading the way

This chapter sets out the UK's approach to maintaining the best talent and how the public sector, across all parts of the UK, can lead by example in addressing the cyber security capability. We acknowledge that there is much more that the public sector can do to achieve this, and we want to understand what the public sector should prioritise to set the most useful examples to industry.

- Are there any specific commitments you feel the public sector in the UK should lead on and adopt in order to set an example for the rest of the UK economy?
- Are you aware of any examples where the UK Government effectively engaged with industry to disseminate information and distil best practice?
- Are you aware of any initiatives or programmes internationally to build cyber security capability that you think would be beneficial if applied in the UK?

Endnotes

Endnotes

- 1 Cyber Skills Immediate Impact Fund
- 2 Pedley, D., McHenry, D., Motha, H., Shah, J (2018). Understanding the UK cyber security skills labour market. Ipsos MORI
- 3 Cyber Security Breaches Survey, (2018). Department for Culture, Media & Sport / Ipsos MORI
- 4 National Cyber Security Centre Annual Review
- 5 Cyber Security Breaches Survey, (2018). Department for Culture, Media & Sport/ Ipsos MORI
- 6 Pedley, D., McHenry, D., Motha, H., Shah, J (2018). Understanding the UK cyber security skills labour market. Ipsos MORI
- 7 Using behavioural insights to improve the public's use of cyber security best practices, (2014). Government Office for Science/ Northumbria University
- 8 Artificial Intelligence Sector Deal, (2018). Department for Business, Energy and Industrial Strategy/Department for Culture, Media & Sport
- 9 Cyber security professionals focus on developing new skills as workforce gap widens, (2018). ISC²
- 10 National Cyber Security Centre Cyber Essentials
- 11 Pedley, D., McHenry, D., Motha, H., Shah, J (2018). Understanding the UK cyber security skills labour market. Ipsos MORI.
- 12 The business and public sector population data are taken from BEIS business population estimates in 2017. These are the latest estimates as of the publication of this report. The charity estimates are taken from the combined total populations across the three charity registers for England and Wales, Northern Ireland and Scotland. For all the extrapolated figures presented here and across the report, Ipsos MORI have rounded to either the nearest 100, or to three significant figures. These figures are of course subject to margins of error, as with all the results from the survey. The margin of error for businesses in this case is ± 4.2 percentage points. This means that the true figure could be between approximately 660,000 and 765,000 businesses.
- 13 Pedley, D., McHenry, D., Motha, H., Shah, J (2018). Understanding the UK cyber security skills labour market. Ipsos MORI
- 14 The survey asked organisations how important it was for them to possess high-level technical skills to carry out a specific range of tasks. For example interpreting malicious code, using cyber threat intelligence tools or platforms and carrying out penetration tests. This was on a scale of 0 to 10, where 10 was essential. For more information regarding the higher-level technical skills that were included please see Pedley, D., McHenry, D., Motha, H., Shah, J (2018). Understanding the UK cyber security skills labour market. Ipsos MORI
- 15 Pedley, D., McHenry, D., Motha, H., Shah, J (2018). Understanding the UK cyber security skills labour market. Ipsos MORI
- 16 These figures are subject to margins of error. In this case, the margin of error for businesses is ± 3.9 percentage points. This means that the true figure could be between approximately 356,000 and 462,000 businesses. Pedley, D., McHenry, D., Motha, H., Shah, J (2018). Understanding the UK cyber security skills labour market. Ipsos MORI
- 17 Pedley, D., McHenry, D., Motha, H., Shah, J (2018). Understanding the UK cyber security skills labour market. Ipsos MORI
- 18 External providers are those that offer IT or cyber security services to other organisations
- 19 Pedley, D., McHenry, D., Motha, H., Shah, J (2018). Understanding the UK cyber security skills labour market. Ipsos MORI
- 20 Pedley, D., McHenry, D., Motha, H., Shah, J (2018). Understanding the UK cyber security skills labour market. Ipsos MORI
- 21 Pedley, D., McHenry, D., Motha, H., Shah, J (2018). Understanding the UK cyber security skills labour market. Ipsos MORI
- 22 Pedley, D., McHenry, D., Motha, H., Shah, J (2018). Understanding the UK cyber security skills labour market. Ipsos MORI
- 23 Pedley, D., McHenry, D., Motha, H., Shah, J (2018). Understanding the UK cyber security skills labour market. Ipsos MORI
- 24 Centre for Strategy and Evaluation Services , (2018). Identifying the Role of Further and Higher Education in Cyber Security Skills Development: A report for the Department for Digital, Culture, Media & Sport
- 25 Centre for Strategy and Evaluation Services , (2018). Identifying the Role of Further and Higher Education in Cyber Security Skills Development: A report for the Department for Digital, Culture, Media and Sport
- 26 Centre for Strategy and Evaluation Services , (2018). Identifying the Role of Further and Higher Education in Cyber Security Skills Development: A report for the Department for Digital, Culture, Media and Sport

- 27 Centre for Strategy and Evaluation Services , (2018). Identifying the Role of Further and Higher Education in Cyber Security Skills Development: A report for the Department for Digital, Culture, Media and Sport
- 28 Centre for Strategy and Evaluation Services , (2018). Identifying the Role of Further and Higher Education in Cyber Security Skills Development: A report for the Department for Digital, Culture, Media and Sport
- 29 Centre for Strategy and Evaluation Services , (2018). Identifying the Role of Further and Higher Education in Cyber Security Skills Development: A report for the Department for Digital, Culture, Media and Sport
- 30 Centre for Strategy and Evaluation Services , (2018). Identifying the Role of Further and Higher Education in Cyber Security Skills Development: A report for the Department for Digital, Culture, Media and Sport
- 31 The Scottish Government
- 32 Centre for Strategy and Evaluation Services , (2018). Identifying the Role of Further and Higher Education in Cyber Security Skills Development: A report for the Department for Digital, Culture, Media and Sport
- 33 National Cyber Security Strategy (2016-2021). HM Government
- 34 Pedley, D., McHenry, D., Motha, H., Shah, J (2018). Understanding the UK cyber security skills labour market. Ipsos MORI
- 35 Cyber Security Body of Knowledge:
 - 36 Response to the Consultation on Developing the UK Cyber Security Profession
 - 37 Revised GCSE and equivalent results in England: (2016 to 2017). Department for Education
 - 38 A level and other 16 to 18 results: (2016 to 2017) - provisional. Department for Education
 - 39 Apprenticeship and levy statistics: (2018). Department for Education
 - 40 Serious and Organised Crime Strategy, (2018). HM Government
 - 41 Global Information Security Workforce Study, (2017). Women in Cyber Security
 - 42 Women in Tech. techUK
 - 43 EMEA Women in Cyber. Deloitte
 - 44 Tech She Can Charter. PwC
 - 45 SheLeadsTech. ISACA
 - 46 Code First Girls
 - 47 Autism facts and history. National Autistic Society.
 - 48 Autism facts and history. National Autistic Society
 - 49 Neurodiversity at work. CIPD
 - 50 Cyber Neurodiversity Group
 - 51 UK Digital Strategy, (2017). Department for Culture, Media & Sport
 - 52 Essential digital skills framework , (2018). Department for Education
 - 53 Statutory Review of Apprenticeship Standards on the Digital Route, (2018). Institute for Apprenticeships
 - 54 FTSE 350 Cyber Governance Health Check Report (2017)
 - 55 Cyber Security Breaches Survey,(2018). Department for Culture, Media & Sport. / Ipsos MORI
 - 56 Small Business Guide, National Cyber Security Centre
 - 57 Cyber Essentials. National Cyber Security Centre
 - 58 Donaldson, S., Stow, C and Hobson, J (2018). UK Cyber Security Sectoral Analysis and Deep-Dive Review. RSM
 - 59 Donaldson, S., Stow, C and Hobson, J (2018). UK Cyber Security Sectoral Analysis and Deep-Dive Review. RSM
 - 60 The registration of interest online form can be accessed via the Cyber Security Skills Strategy page on GOV.UK
 - 61 The call for views online survey can be accessed via the Cyber Security Skills Strategy page on GOV.UK

