Department for
Digital, Culture,
Media & Sport

IMPLEMENTING THE NATIONAL CYBER SECURITY STRATEGY - DEVELOPING THE CYBER SECURITY PROFESSION IN THE UK

GOVERNMENT CONSULTATION

OPEN 19 JULY 2018

CLOSES 31 AUGUST 2018

CONTENTS

FOREWORD BY THE MINISTER FOR DIGITAL AND THE CREATIVE INDUSTRIES

The UK has some of the best cyber security professionals in the world. They play a critical and ever increasing role in not only the UK's 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.

Since the National Cyber Security Strategy was published in 2016, the cyber threat has continued to diversify and grow, bringing in to even sharper focus the need to develop our capability. As our reliance on technology also grows, the opportunities for those who would seek to attack and compromise our systems and data increase, along with their impact. 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 Strategy.

That is why I am delighted to be publishing this consultation which advocates a bold and ambitious approach to creating the environment for, and accelerating the development of, the cyber security profession in the UK. I believe these proposals will help ensure the profession more coherently encourages a broader range of people with the right capabilities to enter the profession, as well as helping those already in it to have their skills and expertise recognised more easily and in a clear and consistent way. The proposals are also designed to help employers and consumers be more confident in the professionalism, capability and integrity of those they employ or those who provide cyber security services.

I am extremely grateful to everyone who has contributed to the development of this consultation so far. We have engaged extensively with existing professional organisations, students, employers, existing cyber professionals and academia. I want to be clear that these proposals are not designed to create an additional membership cost for cyber security professionals to bear or to replace or replicate existing professional organisations. Rather these proposals work with and build on the excellent work and expertise of the existing professional community, to ensure that collectively we can deliver on stretching objectives to develop the profession at the pace required.

We are purposely consulting at this early stage to ensure everyone with an interest in the future of the cyber security profession in the UK can meaningfully and formally contribute. I look forward to hearing your views on the proposals.

MARGOT JAMES MP

INTRODUCTION

The National Cyber Security Strategy (NCSS) 2016-2021 sets out the Government's ambition to ensure there is a sustained supply of the best possible home-grown cyber security talent. One of the key initiatives to deliver is defined as:

> "*developing the cyber security profession, including through achieving Royal Chartered status by 2020, reinforcing the recognised body of cyber security excellence within the industry and providing a focal point which can advise, shape and inform national policy".* [1]

Government engaged extensively with representatives from across the cyber security ecosystem to produce proposals to implement the NCSS outcome and create the environment for the cyber security profession in the UK to develop at the pace required. This engagement included professional organisations in cyber security, cyber security employers, cyber security professionals, academia, charities, small and medium sized enterprises and a wide range of sectors, such as accountancy and financial services, who have an interest in cyber security.

Based on that extensive engagement, this document outlines the progress that has been made so far to develop the cyber security profession in the UK and the remaining challenges. The document then sets out bold and ambitious proposals to create the environment to develop the cyber security profession further. Our starting point has been to recognise the progress made to date and seek not to replicate or replace existing work or structures, but rather to harness, boost, and bring more coherence to the breadth of existing activity.

We believe the implementation of this must be led by the cyber security profession itself, with government's role being to set clear expectations and help kick-start the work. We have therefore defined clear objectives for the profession to deliver by 2021, focused around four themes: professional development, professional ethics, thought leadership and influence and outreach and diversity.

We go on to outline that we believe a new mechanism, a UK Cyber Security Council, which would be independent of government, have organisational membership and be designed and owned by the profession, is required. It is our view that a Council model would be an effective way of helping the existing professional community in the achievement of its aims by bringing more coherence, coordination and

[1] National Cyber Security Strategy 2016 - para 7.19 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

consistency at national level, and across the whole of the cyber security profession, in pursuit of common objectives.

Consulting on these proposals reflects our commitment to ensure everyone with an interest in the profession in the UK can meaningfully contribute to and help shape the policy further. The specific aims for the consultation are to:

- Summarise the government's understanding of the challenges facing the development of the cyber security profession.
- Seek views on objectives for the profession to deliver by 2021 and beyond.
- Seek views on the creation of a new UK Cyber Security Council to help deliver those objectives.

The information below sets out more practical information about how to engage with and respond to the consultation.

WHO IS THIS CONSULTATION FOR?

We are keen for as broad a range of interested parties as possible to engage with and respond to the consultation. This includes, but is not limited to:

- Current cyber security professionals
- Individuals who aspire to work in cyber security in the UK
- Current or prospective employers of, or consumers of services provided by, cyber security professionals in the UK
- Existing cyber security professional organisations, including certification and qualification providers
- Students, recent graduates and adults mid-career who are thinking about cyber security as a career
- Academia
- Other professions which interrelate with existing cyber security professional organisations
- Law enforcement community
- Any other organisations with an interest in cyber security in the UK

Issue date: The consultation was issued 19 July 2018
Deadline: The consultation closes at 17:00 on 31 August 2018.

How to respond: To help us analyse the responses, please use the online portal[2] to respond. In each section of the portal, there is a summary of the corresponding part of this document which represents the full consultation document.

[2] https://dcms.eu.qualtrics.com/jfe/form/SV_5uxqglvphWTsYUl

Enquiries: For questions on how to engage with the consultation process, you can contact the team on: csprofession@culture.gov.uk. Responses to the consultation or about the substance of the policy should be submitted through the online portal. We will not consider correspondence sent to the csprofession@culture.gov.uk inbox as a response to the consultation.

Other ways to respond: If for exceptional reasons, you are unable to use the online system, for example because you use specialist accessibility software that is not compatible with the system, please request a word document version of the form by emailing csprofession@culture.gov.uk and send it back to the same address, or post it FAO Cyber Security Profession consultation team, Cyber Security, DCMS, 100 Parliament Street, SW1P 2BQ.

Additional copies: Additional copies are available electronically and can be downloaded from GOV.UK DCMS consultations.

Next steps: The government's response is likely to be published on GOV.UK in autumn 2018.

CONTEXT AND THE RATIONALE FOR INTERVENTION

There is no set definition of what constitutes a profession but it is generally recognised that it requires preparation/training before entering and members of that profession are trusted by virtue of adhering to a requisite and widely recognised standard of competence, knowledge and ethics. Many existing and established professions have developed over decades and centuries, maturing and responding to societal change and technological developments.

The cyber security profession is relatively new and has developed organically over recent years. It is broad and varied; those working in the cyber security ecosystem are found across multiple disciplines including engineering, technology, business, social science, compliance and law, with a wide range of different competencies. There are many widely recognised cyber security roles - from technical roles like penetration testing through to more strategic and policy positions of Chief Information Security Officers.

In the development of this consultation, we heard about the range of positive activity to develop the profession to its current position. There is a wide range of existing initiatives to attract the next generation of cyber security professionals and to help those already in the profession build their capability and expertise. This has been driven forward by many dedicated individuals and organisations who care deeply about what is best for the profession and want the UK to continue to be a global leader in cyber security.

However, we heard strongly during our pre-consultation engagement that to build on the good work, more needs to be done to create the environment for the cyber security profession in the UK to develop at the pace required. There was a strong sense from many we engaged with that there is no generally accepted, unifying narrative of what makes a cyber security professional. Misconceptions and stereotypes about cyber security professionals remain and we heard clearly that many still consider cyber security to be a complex subject area and a career which lacks clear routes into and through it.

For those already working in the profession and their employers, we heard that the current qualification and certification landscape is hard to navigate, making it difficult to assess the options available and make appropriate, informed choices about career paths or the skills that an organisation requires. There was a strong call for a defined list of certifications and an easy to understand framework of how they all link together, and what capabilities they convey. We heard the existing literature that tries to explain the cyber landscape in the UK reads like a catalogue of diverse initiatives, rather than a narrative of a coherent profession.

Some employers thought this lack of clarity meant they could not easily assess the capabilities of individuals they are employing to perform cyber security roles. With new legislation, such as the Data Protection Act 2018 and the Network and Information Systems (NIS) Regulations 2018, affecting the cyber security ecosystem, it becomes even more important that organisations receive services from a professional they can easily and reliably discern the capability of. The ability to employ an individual with professional qualifications which are reliable and widely recognised also has potential implications for areas like insurance and risk.

There is also more to do to attract the next generation of cyber security professionals and adults who want to transition in to a career in cyber security. Boosting diversity in the sector is a critical thread throughout all of this. There is a range of excellent outreach initiatives, across government and the private sector, but these can sometimes be hard to find or the choice confusing and overwhelming. We heard strongly during pre-consultation engagement that there needs to be better coordination of the outreach offering on behalf of the whole profession. We believe it is also important to work with employers who have tailored entry schemes to draw on best practice and develop much clearer pathways into the profession for the most diverse range of individuals who might have the core capabilities required.

The current landscape is also challenging for existing professional organisations and vendors. Many are unable to articulate the equivalence of their qualifications or certifications in the absence of a common technical framework. Stakeholders we spoke to referenced the excellent work of the existing professional organisations but better coordination and articulation of how their work fits together would mean it could have a greater collective impact. Crucially, we heard that there was no widely recognised and authoritative voice to coordinate and corral views from the whole breadth of the cyber security profession. We heard there was a need for a clearer front door in to the profession to route individuals to the right specialism.

We also consider more needs to be done to harness the collective effort of government and the profession. The National Cyber Security Centre (NCSC), the Department for Digital, Culture, Media and Sport (DCMS) and other departments are currently curating and running a range of initiatives in lieu of a centralised professional function taking them on (for example, certification schemes for both professionals and education). Government will continue to have an active role but we believe greater coherence in the UK's professional landscape will enable a range of initiatives to be led by the profession, thus ensuring their sustainability.

The rapid development of technology and policy development on how we use data and information make these challenges even more pronounced, and the need for action more pressing. The Data Protection Act 2018, for example, is a major step for organisations across the UK and the development of AI and crypto-currencies for example is already demanding new approaches from government and the private sector. Cyber security is a core aspect of all of this. Even more immediately, the report published by DCMS on Secure by Design recognises that while the Internet of Things (IoT) brings huge opportunities for citizens and the UK's digital economy, many internet-connected devices sold to consumers lack even basic cyber security provisions.

We believe it is critical to create the environment to develop the cyber security profession further to address the existing challenges set out above and ensure the UK is well placed to address these new opportunities and challenges.

QUESTIONS

- **1. The summary above sets out our understanding of the profession based on extensive pre-consultation engagement. It sets out challenges around awareness of routes in to and through the profession, the extent to which individuals and employers value the range of qualifications and certifications available and the profession speaking with one, coordinated and coherent voice. Are there any other challenges you perceive in the current cyber security professionalisation landscape that you feel need to be addressed?**
  Free text

ADDITIONAL CONTEXT

WHAT DO YOU MEAN BY CYBER SECURITY?

During our early engagement on the development of the profession, one of the common questions was: ‘what do you mean by cyber security?’ Our early responses emphasised that cyber security is a relatively new and broad domain, and we made reference to the NCSS which 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.”*

Whilst this is a good definition and remains accurate, we acknowledge that it is high level and, for the purposes of a consultation on the profession, in order to organise, action and align activity, we need to be more precise. Acknowledging those common definitions and approaches, the National Cyber Security Programme has undertaken a project to define the foundational knowledge upon which the field of cyber security is built.

The Development of the Cyber Security Body of Knowledge (CyBOK) project[3] is being undertaken by a team of UK academics, led by Bristol University, in consultation with the national and international cyber security sector. During Phase 1 of the project (which was completed in October 2017), the team carried out extensive consultation to define the scope of cyber security. The resultant 19 Knowledge Areas are shown in figure 1 below:

[3] https://www.cybok.org/

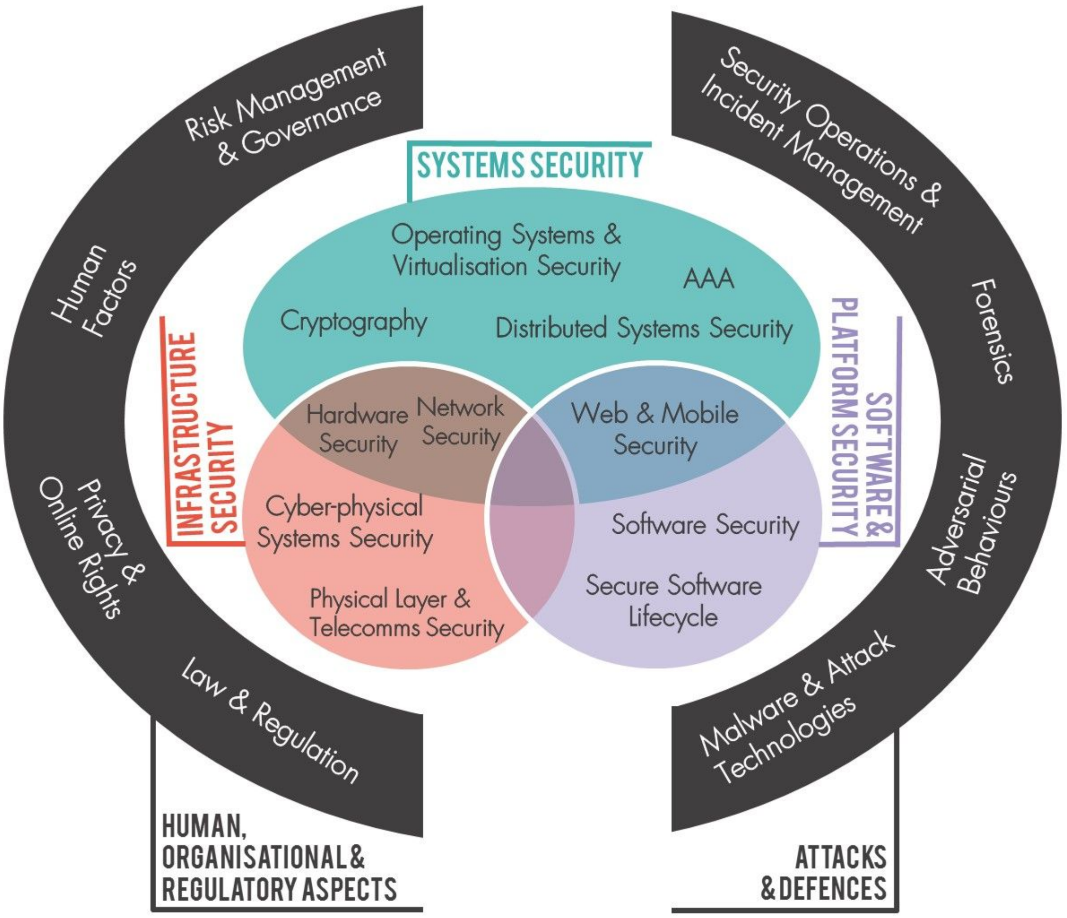
Risk Management & Governance
Human Factors
Privacy & Online Rights
Law & Regulation
HUMAN, ORGANISATIONAL & REGULATORY ASPECTS
SYSTEMS SECURITY
Operating Systems & Virtualisation Security
AAA
Cryptography
Distributed Systems Security
INFRASTRUCTURE SECURITY
Hardware Security
Network Security
Web & Mobile Security
Cyber-physical Systems Security
Physical Layer & Telecomms Security
Software Security
Secure Software Lifecycle
SOFTWARE & PLATFORM SECURITY
Security Operations & Incident Management
Forensics
Adversarial Behaviours
Malware & Attack Technologies
ATTACKS & DEFENCES

Figure 1: The Knowledge Areas that are the foundation of the discipline of cyber security

We believe that this represents the community-consensus view and provides a useful depiction of the field of cyber security. Within the set of Knowledge Areas, it allows for both breadth, incorporating matters of business and IT; and technical depth, acknowledging accepted areas of cyber specialism. We would like to emphasise that as part of this consultation we are not asking for comment on the 19 Knowledge Areas.

The depiction of the 19 Knowledge Areas sets the scope of cyber security to shape approaches for training, standard setting, the dissemination of expert opinion, and the execution of professionalism. Readers should have the CyBOK figure in their minds as they read and comment on this consultation document.

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 develop the profession will be to help align the outputs from these initiatives.

WHY IS GOVERNMENT INVOLVED IN THIS?

In view of the challenges articulated above, and the pressing need to make sure the UK's cyber security workforce has firm foundations to respond to forthcoming opportunities and challenges, we believe there is a strong case for government to act. We have done so by developing an understanding of the main challenges and opportunities as perceived by the different and varied user groups and have used that to develop clear, evidence based objectives and expectations of how we think the cyber profession should develop. This consultation is designed to give interested stakeholders the opportunity to respond formally to proposals.

We have been asked a number of times why government, or the NCSC specifically, does not just lead the implementation of a solution itself. We believe that for the profession to fully represent the needs of the cyber security sector and present a single, clear and authoritative voice on its behalf, it must be independent and objective. The core ingredients for professionalism already exist today in the landscape of existing organisations. We consider that government's role is to help create the environment for the development of the profession, with a view to a Council, if supported by the consultation process, working towards that becoming a self-funding model and being fully independent of government.

A meaningful amount of the National Cyber Security Programme (which implements the NCSS) investment will be available to implement the outcomes of the consultation. This would represent seed-funding to make quick progress on the objectives up until 2021. While the NCSP comes to an end in 2021 and future funding cannot be guaranteed, government will continue to support the resulting mechanism and remains committed to the long term delivery of the overarching strategic outcome.

WHAT DOES THIS MEAN FOR EXISTING PROFESSIONAL ORGANISATIONS AND DON'T SOME ORGANISATIONS ALREADY HAVE A ROYAL CHARTER?

The proposal in this consultation for a new UK Cyber Security Council is designed to help bring more coherence, coordination and consistency, rather than to replace, replicate or compete with existing organisations. The Council's strength will be founded on the credibility and expertise of the existing professional landscape, and we therefore anticipate the Council having broad representation from across the cyber security ecosystem, with a range of different types of organisations playing an active role. This will include, for example, professional bodies, academia, providers of cyber security certifications and qualifications, training providers and other organisations who have had a key role to play in the development of the cyber security profession to this point.

As set out in the NCSS, we also expect the Council to oversee the development of a Royal Chartered status as the gold standard of expertise, excellence and professional conduct for cyber security professionals to aspire to. We do not envisage the Council awarding chartered status to individuals itself, but rather licensing its organisational members to offer a common chartered status to their individual members. That would allow the range of organisations, some of whom may separately have been incorporated by Royal Charter and others who have not, to issue a common chartered status for cyber security overseen by the Council.

We have developed this model by engaging with partners across the cyber security ecosystem and believe it represents an effective way of ensuring that the broad range of existing professional organisations who cover the different specialisms in cyber security have the opportunity to play a meaningful role in the Council and award chartered status to their members.

PROPOSALS

OVERVIEW

As set out above, based on our extensive engagement we have defined clear objectives for the profession to deliver by the end of the National Cyber Security Programme window in 2021. These are focused around four themes: professional development, professional ethics, thought leadership and influence and outreach and diversity. The consultation goes on to set out that we believe a new UK Cyber Security Council is required to help ensure these objectives are delivered.

OBJECTIVES

1. Professional Development

Supporting the continued professional development of those already working in or aspiring to work in cyber security, and helping employers and consumers make more informed decisions about the cyber security capability they need, is at the heart of what we are setting out to achieve.

We believe there needs to be a system that supports and guides individuals in to and through their careers, and also provides them with incentives to stay within cyber security. We believe getting this right will bring greater recognition and clarity to the profession, with a career in cyber security becoming more recognised and structured in the same way as more established and mature professions.

The first few years in a cyber security career are vital. We believe there need to be more coherent early career offerings, helping individuals choose where they may want to focus or specialise and gain the experience needed. For those who have been active in the profession for a number of years, but who do not hold relevant academic or professional qualifications, we believe there is also a need for a commonly adopted framework through which individuals can demonstrate their skills and experience in a way that others understand. There should be clarity and direction around how everyone, at whatever level, can progress in their chosen career paths, and transition to other areas of cyber security based on their capability.

The professional development provision needs to be of a requisite and common standard, agreed across all specialisms within the broader cyber security domain and should apply to all cyber security professionals, from risk managers, penetration testers through to threat analysts and cryptographers.

A more coherent approach to professional development is crucial for organisations employing or using the services of cyber security professionals. Organisations need to have the confidence that individuals they entrust to secure their information have the capabilities they say they do. While there are many credible vocational qualifications and academic certification routes into the profession, we consider there remains a lack of credible information supporting what those qualifications actually mean and the true capability and expertise someone who possesses some of those qualifications has. Our pre-consultation engagement told us that many organisations, particularly those taking their first steps in securing their information, can be confused by the array of qualifications and certifications.

For certification and training providers, while there are various skills frameworks, there is no agreed, adopted or widely recognised framework to make it easy to understand what capabilities and expertise that qualification/certification represents. This can be both commercially confusing and prove to be expensive for organisations and individuals pursuing a career in the cyber security profession.

We have developed specific objectives we believe would further develop the cyber security professional development landscape by 2021. These are:

By end of 2019:

- The early development and alignment of a coherent set of career specialism pathways, both into and through the cyber security profession, clearly identifiable and widely agreed across the cyber security sector and with government. This should include the alignment and coordination of the vast range of valuable professional qualifications and certifications which spans both vocational and academic certification already available. It should also allow for inclusion of future qualifications that may be introduced to support legislation and technological advancement.

- The foundation of these activities will be the use of the Cyber Security Body of Knowledge (CyBOK), a comprehensive body of knowledge to inform and underpin standards, career structures, education and professional training for the cyber security sector.

By end of 2020:

- Developed proposals for, and early implementation of a common Royal Chartered Status for individuals to aspire to across the range of cyber security specialisms. This should represent the gold standard of expertise, excellence and professional conduct in the profession, and be integrated into the framework of existing qualifications and certifications. Cyber security professionals should have a clear and consistent view about how they progress towards obtaining the status.

By mid-2021:

- A framework, agreed across the profession, setting out the comprehensive alignment of career pathways through the profession, leading toward a nationally recognised career structure adopted by the whole cyber security sector across the UK.

- As part of that framework, full implementation of routes to chartered status for cyber security professionals across all specialisms in cyber security.

QUESTIONS

- **2. To what extent do you agree or disagree that the objectives on professional development are ambitious and stretching enough to respond to the challenges set out in the case for intervention?** *Strongly agree, agree, neither agree or disagree, disagree, strongly disagree, don't know*

- **3. To what extent do you agree that the concept of creating a chartered standard for cyber security professionals would be an effective way of recognising cyber security professionals' excellence and expertise in their fields?** *Strongly agree, agree, neither agree or disagree, disagree, strongly disagree, don't know*

2. Professional Ethics

The nature of a cyber security professional's role raises a series of ethical considerations and responsibilities. Employers place enormous trust in their cyber security specialists because those individuals often have privileged access to highly sensitive information, as well as the operation of critical business systems and processes. Those working in the sector may encounter breaches of applicable laws and regulations and have important obligations involving law enforcement.

Our pre-consultation engagement showed strong support for a cohesive Code of Ethics which is adopted and applied across the different specialisms and qualifications/certifications in cyber security. Many other sectors have ethics statements; for example, the Engineering Council and the Royal Academy of Engineering have established a short list of ethical principles that members are required to abide by, including:

> *Accuracy and rigour, Honesty and integrity, Respect for life, law and public good and Responsible leadership: listening and informing.*

We believe a widely adopted and agreed Code of Ethics for the whole of the cyber security profession is one of the foundation stones to ensure individuals have a clear framework and guiding principles to exercise professional judgement. It would enable organisations and individuals to share their experience in order to achieve a clearer overview of good ethical practice and to reduce exposure to risk in this area.

By end of 2019 we would expect:

- A draft Code of Ethics, agreed voluntarily between participating cyber security professional organisations, which is applicable across the whole of the cyber security sector. It may cover, for example:
    - The professional and ethical obligations cyber security professionals have in relation to clients and services they provide, to ensure they work with integrity at all times.
    - The requirement for the advice and conduct of professionals to be consistent with applicable laws and regulations (e.g Network and Information Systems Regulations 2018 and the Data Protection Act 2018).
    - Obligations vis-a-vis reporting to law enforcement.
    - An expectation that everyone should be treated fairly and without discrimination.

- Draft guidance on the limits of a professional's personal responsibility if their design, product or data are misused by others; whistleblowing and responsible disclosure.

By end of 2020:

- Early implementation of the Code of Ethics and proposals on how to consistently monitor and enforce the Code within signatory organisations.

QUESTION

- **4. Do you think having a commonly agreed and adopted Code of Ethics for cyber security professionals for all specialisms is a good idea?** *Yes/No/Don't know*

- **5. Why do you think it is or is not a good idea to have a commonly agreed and adopted Code of Ethics for cyber security professionals of all specialisms?** *Free text*

3. Thought Leadership and Influence

The UK has a strong and vibrant cyber security ecosystem, ranging from innovative start-ups through to world leading cyber security businesses and academic institutions, all of whom play a critical role developing creative and innovative solutions to address the cyber challenges of today and tomorrow. Government continues to play a key role too - using its convening power to bring in the wider ecosystem to develop policy and with the NCSC as the UK's technical authority.

The cyber security professional community is knitted into and throughout each of the different parts of the cyber ecosystem so having a strong voice that can speak and advocate on behalf of the whole profession is critical. We heard that while there are many credible voices already representing parts of the profession already, the collective impact of the profession can be reduced by a lack of coordination or alignment.

A key theme we heard in pre-consultation engagement was the appetite for strong and visible leadership, which can coordinate the views of and speak authoritatively on behalf of all of the different specialisms and organisations in cyber security. This is crucial not only for speaking coherently to the different parts of the cyber security ecosystem, including government, but also, given the importance of cyber security to all sectors of the UK economy, for more effective reaching out to and development of links with other sectors. We believe this coordinated leadership will help those other sectors define their cyber capability requirements better. Recent cyber attacks, which affected core public services and used Internet connected devices to breach private companies, reinforce that requirement.

Cyber security is a global sector and many existing organisations already have strong international links. We want to ensure that the UK's cyber security professional community continues to develop its integration within the wider international community. This is about the profession in the UK being able to draw from best practice in other countries who are investing in and developing their cyber security ecosystems. We need to ensure that we are taking steps to identify innovation and proactively learn from international best practice so that the UK remains a global leader. Furthermore, we need to make sure frameworks and qualifications used by cyber security professionals in the UK are recognised as the gold standard internationally.

We believe the objectives set out below would deliver that more coordinated and visible thought leadership and influencing function on behalf of the whole profession:

During 2019:

- An agreed and adopted vision statement and roadmap for how the profession as a whole will provide coordinated leadership and influence other sectors and government in the best interests of the profession.

By end of 2020:

- The profession as a whole is coherently driving and shaping public opinion about cyber security in the UK, and working collaboratively with government to develop cyber security policy.

- The different specialisms in cyber security are, in a coordinated way, developing collaborative partnerships internationally and ensuring UK alignment at an international level.

- An agreed strategy, developed across the profession, to define and strengthen relationships with other professional sectors with interests in cyber security – e.g. law, insurance, HR, etc. as well as international partners.

- Working with government, industry and academia to support and promote effective and world-leading cyber security research, practice and education.

By end of 2021

- Coordinates thinking and produces proposals, on behalf of the different specialisms within the profession, to further strengthen the profession. This could, for example, include issues such as regulation of cyber security professionals and a licence to practise.

QUESTIONS

- **6. To what extent do you agree or disagree that the objectives on thought leadership are ambitious enough to respond to the challenges set out in the case for intervention?** *Strongly agree, agree, neither agree or disagree, disagree, strongly disagree, don't know.*

- **7. Do you think there is a requirement for better coordination to ensure there is a coherent and independent leadership voice on behalf of the whole profession?** *Yes/No/Don't know*

- **8. Are there any other policy or professional development issues where you think the profession should lead on the development of an agreed position?** *Free text.*

4. Outreach and Diversity - Developing The Next Generation

The way the profession reaches out to those seeking to join the profession, particularly the next generation of cyber security professionals, is crucial to the sustainability of the profession. Cyber security needs to be seen as a viable and attractive career option for a greater, more diverse range of people. For that to happen, we believe the perception of a career in cyber security needs to change. The profession must show opportunities for flexible, rewarding and hugely interesting work not only to those who might traditionally be interested in cyber security, but a much wider range of people who have the core skills and capabilities to succeed.

There has been much progress already. There is a range of initiatives where government has partnered with and drawn on expertise in industry, such as Cyber First, Cyber Discovery and the recently launched Cyber Security Immediate Impact Fund, all aimed at developing the skills pipeline and boosting diversity. There has also been progress on a wide range of other excellent initiatives and interventions outside of government which seek to help develop the pipeline. But it was clear from our initial engagement that to build on this progress, we must focus more widely than on those with a computer science or cyber security degree - the next generation must include those already in work in another profession and school leavers.

There is a strong appetite for a more cohesive and visible outreach function on behalf of the whole cyber security profession. We believe it is essential that the cyber security profession works together on this to develop innovative and creative solutions and to scale up, increase the pace of, and drive better coordination of existing initiatives. This is about boosting and helping innovation rather than stifling it, and the cyber security profession is central to this effort. We have defined a number of objectives below which we consider the profession should lead to deliver a more coherent outreach offering:

By end of 2019:

- A clear mission statement, aligned with the government's upcoming Cyber Security Skills Strategy, agreed across the profession, on how to develop the next generation of cyber security professionals and boost diversity in the sector.

- Work with government to build a clear and authoritative evidence base on cyber security skills in the UK.

- Clear evidence of identifying links and partnerships between initiatives and amplify the good work done by others to ensure that there are pipelines of activities and opportunities for those of all ages who are looking to develop their skills or join the sector.

By end of 2020 (indicative - subject to discussion with relevant government departments):

- Working with government, production of a roadmap for transition to the profession of relevant government run skills/capability building initiatives. This should set out a plan for how these initiatives will be sustainable without government funding.

- Establishment of a national network of industry, government and educational sector partners to provide nationwide events to attract people into the profession, including all under-represented groups.

By end of 2021:

- Following agreement with government partners, the potential transition of other initiatives from government to the profession.

QUESTION

- **9. To what extent do you agree or disagree that there is a requirement to produce a clear mission statement, agreed across the whole cyber security profession, on how the profession will develop the next generation of cyber security professionals?** *Strongly agree, agree, neither agree or disagree, disagree, strongly disagree, don't know.*

DELIVERING THOSE OBJECTIVES BETWEEN NOW AND 2021 - A NEW COUNCIL

We believe the objectives set out above are ambitious and stretching and delivering them needs to be a collaborative effort by the whole cyber security sector. As previously noted, our starting point has been to recognise the excellent work existing professional organisations have done and consider how a new mechanism can help in the achievement of their aims by bringing more coherence, coordination and consistency at a national level, and across the whole cyber security profession, in pursuit of common objectives. We do not believe that it would be sensible or that it is necessary to create a new professional body that replaces or replicates existing professional organisations.

Our central proposal is for there to be an independent **UK Cyber Security Council** to drive delivery against the objectives above. We envisage the Council would have organisational rather than individual membership and be made up of existing professional bodies and other organisations with an interest in cyber security. It is intended to bring coherence to a broad range of specialisms or constituent organisations while allowing those specialisms to maintain their unique offerings. We want to be clear that this is not about duplicating existing organisations, or expecting individuals to join an additional organisation.

To be viable and have the buy-in required, the Council would need to be designed, owned and operated by the sector, with broad support from across the ecosystem it seeks to represent. We have purposely not been overly prescriptive about how it might be implemented, but have defined a series of fundamental attributes and functions we believe the Council should develop and perform:

Represents the breadth of the Cyber Security profession spanning academia, industry, government and existing professional bodies, and with geographical remit for the whole of the UK

- The Council would need to have broad and proportionate representation from across the cyber security ecosystem. This would include existing professional organisations, academia, cyber security business and employers and government. This would ensure it is a collaborative endeavour. The Council should not seek to replicate or replace existing professional organisations and should seek to define its role as not being in competition to other, related Councils or umbrella organisations.

- In order to have credibility, both nationally and internationally and appeal to the breadth of the profession, the Council must ensure all areas and specialisms within cyber security are represented. The illustrative diagram the NCSP funded CYBOK project has produced demonstrates a view of the scope of cyber security[4]. We would envisage any new mechanism demonstrating how it could represent these functions.

- We envisage the Council acting as a 'front door' into the profession, helping those new in to the profession to understand which existing professional body or organisation would best serve their interests.

- We would expect the Council to work with UK government, including with the NCSC as the technical authority, and the devolved administrations, to ensure the Council has appropriate representation and reach for the whole of the UK, and complements existing structures in each part of the UK.

A new not-for profit organisation working for the public benefit

- The aim of the new Council should be to work for the public benefit and be a not-for-profit organisation. We would expect the Council to work with government in its early stages to define its status and trajectory. Establishing the Council as a new legal entity will be one of the first key milestones and will emphasise its role as a distinctive focal point for the profession.

Self-sustaining intellectually and financially

- The Council would need to become self-sustaining intellectually and financially after the government funding window. We believe this is a realistic ambition given the significant scope to design and shape the Council, and the benefits we believe it would bring to the profession. We would expect the Council to quickly work with government and industry to develop a viable model for financial sustainability, and develop an agreed and robust approach for governance during the initial period of government funding. These might include exploring a levy system using organisational membership fees or other contributions from the wider cyber ecosystem.

Provides strategic and executive leadership for the whole profession

- We believe the Council would need to have strategic and executive leadership to establish and reinforce the role of this endeavour within the profession in the UK and internationally. We believe it would also help ensure delivery momentum against the objectives set out above and serve to reinforce links to different professions who have a stake in cyber security. This strategic

[4] CyBOK diagram - https://www.cybok.org/media/downloads/CyBOK_clusters_-_Final.jpg

leadership role would also be able to engage businesses and other organisations to advocate on behalf of the whole profession.

Oversight of the development of a chartered standard for Cyber Security professionals

- We would expect the Council to oversee the development of a chartered standard for cyber security professionals to aspire to. As set out above, we do not envisage the Council directly issuing chartered status to individuals, but rather it would give the authority or licence for constituent organisations (who would generally specialise in different core skills) to be issuing bodies and grant chartered status to their members who met the requisite standard. The Council would have a key role to play in setting that standard, ensuring its consistency across the different specialisms and ensuring it was implemented properly.

- A number of possible ways could achieve implementation of chartered status for cyber security professionals. We remain open minded but believe it is crucial it becomes visible and widely recognised as the gold standard of professional competence and capability for cyber security professionals.

Networking and cross-specialism development

- The Council would be well placed to help drive even greater access to networking opportunities for members of constituent organisations. Many existing professional organisations already do this but having a wider and more diverse network would, we believe, help challenge and motivate individuals, helping them make the most of opportunities in order to progress their careers and move in to different specialisms.

As part of our extensive pre-consultation engagement, we considered a range of other options on how to deliver the objectives set out above. This started at the do nothing option, right through to recommending a fundamental realignment of the professional landscape in the cyber sector, which could involve elevating one of the existing organisations to become the de facto Professional Body for the whole of cyber security.

We believe that the existing landscape needs to be more coordinated and coherent to deliver a stretching set of objectives, so consider doing nothing is not a viable option. Elevating one or more existing organisations to lead the profession would not bring coherence and integrating the products/services of other organisations outside its membership and could prove difficult, undermining the ability to achieve the objectives set out above. A lighter touch grouping of organisations, or a coordination group with no executive leadership or capacity to deliver things itself would bring some more coherence to the profession but would not, in our view, be sufficient to deliver the stretching objectives. Furthermore, a loose federation is unlikely to be a legal entity and would therefore be unlikely to be able to receive government seed-funding.

We believe there is a strong case to create a UK Cyber Security Council and that it strikes the right balance by doing something ambitious that can deliver on stretching objectives, while also acknowledging the significant progress that has been made to date by existing professional organisations. Government is prepared to offer a meaningful amount of support and also offer schemes and services that will kick start the development of the Council.

This consultation is designed to help Government better understand how the Council might be implemented in a way that ensures it is viable and sustainable in the long term, while also being able to deliver on stretching and ambitious objectives by the end of the NCSP and beyond.

QUESTIONS

- **10. Do you think that a new UK Cyber Security Council is an appropriate way of delivering on the objectives set out above in the consultation document?** *Yes/No/Don't know*

- **11. How much do you think it would cost to design and implement the Council between now and 2021?** *Less than £100k, between £100k-£500k, between £500k-£1m? Between £1m-£2m? Between £2-3m? More than £3m? Do not know/unsure.*

- **12. To what extent do you agree or disagree that it is viable for a new UK Cyber Security Council to become self-sustaining financially by the end of 2021?** *Strongly agree, agree, neither agree or disagree, disagree, strongly disagree, don't know*

- **13. Why do you think that it is or is not viable for a new UK Cyber Security Council to become self-sustaining financially by the end of 2021?** *Free text*

- **14. Are there any other attributes you think would be key for the new Council to include?** *Free text*

SUMMARY AND NEXT STEPS

This consultation is your opportunity to help shape the future of the cyber security profession in the UK. We encourage anyone with an interest in cyber security in the UK to read and respond. The consultation will be open until 31 August 2018 after which government will issue a response which we intend to publish around autumn 2018.

This response is likely to either constitute or be issued in parallel with a detailed set of requirements and an invitation to bid or apply for government funding to lead the design and implementation of what comes out of the consultation and deliver the objectives for the remainder of the National Cyber Security Programme (March 2021). All proposals would be evaluated against published criteria and requirements, and an assessment made to select the successful proposal. The full criteria will be published following the consultation period and response but it is likely proposals will need to show they can command broad support across the cyber security professional development landscape and wider cyber ecosystem.

Summary of Questions
Please note the questions below are for reference only. All consultation responses should be submitted via the online survey.

1. **The summary above sets out our understanding of the profession based on extensive pre-consultation engagement. It sets out challenges around awareness of routes in to and through the profession, the extent to which individuals and employers value the range of qualifications and certifications available and the profession speaking with one, coordinated and coherent voice. Are there any other challenges you perceive in the current cyber security professionalisation landscape that you feel need to be addressed?** *Free text.*

2. **To what extent do you agree or disagree that the objectives on professional development are ambitious and stretching enough to respond to the challenges set out in the case for intervention?** *Strongly agree, agree, neither agree or disagree, disagree, strongly disagree, don't know.*

3. **To what extent do you agree or disagree that the concept of creating a chartered standard for cyber security professionals would be an**

effective way of recognising cyber security professionals' excellence and expertise in their fields? *Strongly agree, agree, neither agree or disagree, disagree, strongly disagree, don't know*

4. **Do you think having a commonly agreed and adopted Code of Ethics for cyber security professionals for all specialisms is a good idea?** *Yes/No*

5. **Why do you think it is or is not a good idea to have a commonly agreed and adopted Code of Ethics for cyber security professionals of all specialisms?** *Free text*

6. **To what extent do you agree or disagree that the objectives on thought leadership are ambitious enough to respond to the challenges set out in the case for intervention?** *Strongly agree, agree, neither agree or disagree, disagree, strongly disagree, don't know*

7. **Do you think there is a requirement for better coordination to ensure there is a coherent and independent leadership voice on behalf of the whole profession?** *Yes/No/Don't know*

8. **Are there any other policy or professional development issues where you think the profession should lead on the development of an agreed position?** *Free text*

9. **To what extent do you agree or disagree that there is a requirement to produce a clear mission statement, agreed across the whole cyber security profession, on how the profession will develop the next generation of cyber security professionals?** *Strongly agree, agree, neither agree or disagree, disagree, strongly disagree, don't know*

10. **Do you think that a new UK Cyber Security Council is an appropriate way of delivering on the objectives set out above in the consultation document?** *Yes/No/Don't know*

11. **How much do you think it would cost to design and implement the UK Cyber Security Council between now and 2021?** *Less than £100k, between £100k-£500k, between £500k-£1m? Between £1m-£2m? Between £2-3m? More than £3m? Do not know/unsure*

12. **To what extent do you agree or disagree it is viable for a new UK**

Cyber Security Council to become self-sustaining financially by the end of 2021? *Strongly agree, agree, neither agree or disagree, disagree, strongly disagree, don’t know*

13. **Why do you think that it is or is not viable for a new UK Cyber Security Council to become self-sustaining financially by the end of 2021?** *Free text*

14. **Are there any other attributes you think would be key for a new UK Cyber Security Council to include?** *Free text*