Wilton Park

Report: Securing technology: sustaining a high quality cyber security workforce

Monday 16 – Wednesday 18 September 2024

In association with
UK Department for Science, Innovation and Technology (DSIT), TechUK and the UK Cyber Security Council

In association with

techUK

UK CYBER SECURITY COUNCIL

Report:
Securing technology: sustaining a high quality cyber security workforce

Monday 16 – Wednesday 18 September 2024

In association with
UK Department for Science, Innovation and Technology (DSIT), TechUK and the UK Cyber Security Council

Executive summary

The cyber security workforce is undergoing a process of professionalisation. At present, countries are largely approaching this domestically with limited international collaboration or coordination. This report reflects discussions around cyber security professionalisation through seven themes:

- The nascency of the cyber security profession
- Balancing the benefits of global harmonisation versus localisation
- The enduring relevance of cyber security in new technologies
- The powerful social message that the cyber security profession helps make the world a better place
- Nurturing the cooperative cyber security community
- Opportunities to use accreditations to bridge the experience gap
- Bringing underrepresented voices into the discussion.

These themes act as hooks for recommendations for the international community developing the cyber security profession. There are six recommendations:

- Creating a shared glossary of profession terms for common understanding
- Building an understanding of similarities and differences in countries' approaches to setting standards for cyber security workforces
- Setting a common baseline for the minimum quality standard for cyber security professionals
- Establishing an approach to make national frameworks and standards interoperable

- Establishing a plan for both private and public sectors to adopt common frameworks and standards
- Promoting efforts to encourage countries to join the professionalisation process and tracking progress towards professionalisation

All of the above is underpinned by a requirement for further research in cyber security skill requirements and labour markets.

The Nascency of the Cyber Security Profession

Cyber security as a formalised profession is a relatively new concept. For example, the UK Cyber Security Council, a professional body, was created in 2021, and Ghana's regulation of cyber professionals was introduced in 2020. These initiatives, intended to organise and manage the cyber security profession in their respective countries, are among the strongest national actions taken to formalise the profession, yet are both less than five years old. Compared to other recognised professions such as accountancy, medicine, or engineering, which have decades or even centuries of professional history, cyber security is only in its infancy of professionalisation. However, the idea of cyber security professionals is not new. People have been working to secure technologies and data long before "cyber security" entered the professional vocabulary. Industry veterans recognise terms like "IT security" and "information assurance" which were associated with cyber-like roles. Meanwhile, the US National Institute of Standards and Technology has had a computer security programme since 1972. Cyber security therefore has a rich history of practice to draw on in developing its profession. So while the role of protecting digital and physical assets is not new, cyber security does come with a lexicon which is perhaps more nuanced than its predecessors and this language is new to many business leaders who seek to understand the relevance and impact of cyber security in their organisations.

The nascency of cyber security as a distinct profession offers an opportunity to create common understanding through a shared glossary of terms. The international community would be well-served by an agreed list of terms that underpin the profession. This glossary is not intended to define technical cyber security terms, but instead clarify shared understandings of terms related to professionalisation, such as "skill", "role", and "accreditation." The glossary will enable people working in cyber security or looking to work in cyber security, as well as those designing training courses and educational programmes, to draw on the same building blocks regardless of what country they are operating in.

Harmonisation versus localisation

Countries are at different stages of the journey to cyber security professionalisation. Some, such as the aforementioned UK and Ghana, have already made significant policy interventions to professionalise their cyber security workforces. Others are at earlier stages in the process, and with desired end states that do not necessarily replicate across geographies – for example the role of a government in regulating the profession. These differing approaches, and the mismatched stages of the professionalisation process, combine to create tension between desires for harmonisation versus localisation of professional standards. Global harmonisation would enable workforce mobility, improve accessibility through transparency, and unburden cyber security professionals from competing standards – for example, international recognition of education and training limits the need for a cyber security professional to acquire multiple versions of the same accreditation for different jurisdictions. On the other hand, localisation recognises that countries are different (politically, economically, demographically etc.) and there is no one approach that fits all; local standards serve local needs. A piece of policy innovation that addresses a problem in one country may not work in other countries. For example, through its labour market research, the UK knows that cyber sector businesses there have large gaps in digital forensics and cryptography and communications security skills[1]. Other countries are likely to have gaps in other skillsets and would therefore look to target policies differently.

Alleviating the tension between harmonisation and localisation requires an approach that affords flexibility, and this can be achieved through modularity. By structuring professionalisation in modules, countries can select modules that suit their needs to build a locally-targeted professional cyber security framework while still adhering to internationally agreed standards. The work and coordination required to build and agree modules (and keep them up to date) is non-trivial, especially across a diverse international community, but would realise the benefits of both harmonisation and localisation. To create this modularity, three cornerstones are required. First, a glossary of shared terms as previously outlined. Second, an agreed baseline for the minimum quality standard for a cyber security professional. Such a standard would

[1] https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2024/cyber-security-skills-in-the-uk-labour-market-2024

ensure that any cyber security professional meets a threshold of competence; if countries want to set their local standard higher that is fine, but an agreed baseline acts as a backstop to enable harmonisation. Third, interoperability between professional frameworks that are currently extant or being developed. As described, some countries are already far into the professionalisation journey and unable to begin again from scratch. For modularity to function, existing frameworks need to be made interoperable through actions like mapping frameworks to each other and recognising frameworks at bilateral or, ideally, multilateral levels. Publicising the results of such mapping exercises and recognition agreements is crucial, so that countries developing frameworks can align with existing frameworks in an agile way. It should also be acknowledged that accreditation organisations can be inundated with mapping requests and consideration should be made to involve others who can undertake such activities, for example academia.

Relevance of cyber security in new technology

Cyber security is an inherently technological subject. It concerns the protection of physical assets (servers, computers, mobile devices), digital assets (data) which reside on or can be accessed via physical devices, and the networking infrastructure which connects devices and through which data flows. While there is great value in approaching cyber security from non-technical angles provided by social sciences and the humanities, it would be futile to attempt to completely decouple cyber security from technology. And, despite its history, it is all too easy to think of cyber security as inexorably tied to contemporary technology. In fact, the opposite is true: technology is ephemeral, but cyber security is constant, though not unchanging. As new hardware, software, and protocols are developed, the requirement for cyber security remains, even if the details of how to implement it changes. New technology does not invalidate cyber security, indeed new technology entrenches the need for cyber security. Artificial intelligence (AI) may be a new technology particularly relevant to cyber security skills, as the ability to automate routine tasks could decrease the need for entry level cyber security roles. But like any other new technology, AI also requires security – it must be developed with security-by-design and integrated in existing systems in a security-conscious manner. There is therefore an open question about the extent to which AI decreases cyber security roles versus augmenting roles to different skillsets.

Amongst the constantly shifting technological landscape, it is critical to avoid becoming distracted by the latest developments. New technologies tend to capture

not only the public imagination, but also the attention of senior government leadership and corporate executives. This has certainly been borne out with AI, where rapid technological development has been followed by rapid policy directives to devote significant national and international effort – not always misplaced – to shepherd and harness the technology. But AI is not the first, and certainly not the last, technology that will go through this cycle. Remembering that cyber security will remain a constant requirement is crucial to maintaining an appropriately skilled workforce, ensuring that technologies are developed and deployed safely and securely. To aid with this at an international level, it would be useful to have a shared understanding of countries' approaches to setting standards for cyber security workforces. There will be differences and similarities in the factors countries take into account when setting workforce standards. Knowing why and how these factors are relevant in some contexts will help countries assess which factors are relevant to them, and perhaps discover factors not previously accounted for, enabling them to modularly approach setting their own cyber security workforce standards.

The social message

Because of its basis in digital technology and historical links to hacking communities, cyber security is often unfairly maligned as a subject only accessible to a small subset of technical nerds and social recluses. This has hurt the public image of cyber security, impacting its attractiveness as a profession. People are unlikely to want to become cyber security professionals if they cannot see people like themselves in cyber security roles. Perhaps more crucially, people are unlikely to be attracted to cyber security (at least not for the right reasons) if the subject is solely associated with breaking into computer systems. It is unfortunate that public perception is skewed this way because cyber security has powerful positive social messages to convey. Cyber security is about fixing things that are broken, enabling new technologies to flourish, empowering communities and businesses online, protecting people from malicious actors, and catching those malicious actors. It is, at its core, a profession that helps make the world a better place. Contrary to its historical image, the cyber security profession should be associated with large amounts of kudos, like medicine or engineering.

There are opportunities to amplify this social message and thereby increase the attractiveness of the cyber security profession. In recruitment campaigns for job roles and training programmes the social message should be included as a core element of the benefits of working in cyber security. Similarly, educational courses should include the positive social functions of cyber security as part of the ethical considerations

many of these courses already cover, and the content should be upfront at the start of a course to set the tone from the beginning, not an addendum at the end. Moreover, when countries consider their approaches to setting standards for cyber security workforces, the social message can be incorporated as part of a standard. Exactly which social messages will resonate with local audiences may differ between countries, but having a selection of messages to choose from that have been used elsewhere would be beneficial when setting standards.

Community

Cyber security is both an art and a science. As an art, there are subjective elements which constitute 'best practice' for one organisation (or industry sector, or geographical region etc.), but objective universal best practices are difficult to establish because risk profiles differ. On the other hand, as a science, cyber security is also a process of discovery and testing – skilled practitioners building shared knowledge about technologies and those who use them. These practitioners learn from each other, often brought together by common causes (see social messages) to form a community of professionals. The cyber security community, like scientific professions it wants to emulate, is by its nature cooperative rather than competitive. The community as a whole has more to gain by members improving collectively, than members gain by improving individually. This means members share knowledge and experiences to enrich others, lifting the community at large and making life difficult for malicious actors. The community spirit is the embodiment of the social messages cyber security has to offer. Community can also be a factor in improving diversity in the cyber security workforce, where women and people from ethnic minority backgrounds tend to be underrepresented[2]. Community can help inspire and guide new workforce entrants from these backgrounds through role models and mentoring.

To take advantage of the community aspects of the cyber security profession, two things are required. Firstly, cyber security workforces in the public and private sectors should be shaped by the same frameworks and standards. At present, the private sector cyber security workforce has largely grown and organised itself organically, driven by market forces. Conversely, public sector workforces are more likely to be shaped by – or at least more likely to be compelled to adopt – frameworks and

[2] https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2024/cyber-security-skills-in-the-uk-labour-market-2024

standards which have been produced or approved by central governments. But this risks creating two communities; and the benefits of having a community could be better realised by simplifying from two to one. Agreeing a plan for domestic adoption of frameworks and standards between private and public sectors would help toward this simplification. Secondly, there is a need to track uptake and impact of these efforts. The strength of the community grows with more members, so active promotion of international efforts towards cyber security workforce professionalisation and tracking increased membership is required to maximise impact. Spreading the message about efforts at large fora such as the Global Cyber Capacity Building Conference in Geneva in May 2025 is likely to raise awareness and encourage new joiners[3].

Certification as bridge

There are many routes for an individual to become a cyber security professional. Some people enter the workplace straight after school, with minimal cyber security expertise, and develop on the job. Others study university degrees in cyber security or computer science to gain relevant knowledge before joining the workplace, while yet others study degrees in entirely different subjects which give them transferrable skills, and subsequently work in cyber security roles. Some people transition into cyber security roles after working in adjacent areas, and some people change careers entirely to become cyber security professionals, sometimes accompanied by spending time upskilling on training courses. In many of these routes, an individual's first role in cyber security is likely to be entry-level. However, the amount of entry-level job seekers outnumbers the entry-level roles available. It is difficult to generate more entry-level jobs so the challenge becomes how job candidates can get experience in order to apply for roles at other levels, without actually getting work experience – a classic chicken and egg scenario. Professional certification may provide part of the solution to the problem. Where education at school and university normally focuses on knowledge, employers often want provable practical skills to indicate that a candidate is job-ready. Professional certificates provided by ISACA, SANS, CREST, CompTIA, ISC2, SFIA, and others are intended to provide assurance that the certificate-holder has both knowledge and skills in the area covered by the certificate – some more specific and some more general. It may therefore be possible to position certifications

[3] https://gc3b.org/

as a bridge in lieu of experience. Additionally, the certification bodies themselves can be bridges within the cyber security community. Because they have relationships with both employers and (prospective) employees they can potentially help connect those who need skills with those who have skills.

For certification to fulfil this potential, a couple of supporting actions are required. Firstly, the aforementioned baseline for a minimum quality standard of cyber security professionals. The baseline would normalise certificates so that no certificate holders fall below the minimum standard, even if most holders would be significantly above the standard. This helps employers understand what knowledge and skills, at a minimum, they can expect to get from a certificate holder. Crucially, a baseline agreed at international level will improve portability of certificates between countries, enhancing the current international recognition of certificates and saving certificate-holders from needing to acquire multiple versions of certificates. Secondly, the interoperability of professional frameworks. Activities like mapping and recognition, as previously mentioned, should include the role of certifications within each framework so that it is well publicised and understood by policymakers, employers, and employees. Ideally this can be done at a granular level down to individual certificates, although such efforts would need regular updating to account for certifications being redesigned in response to market requirements.

Underrepresented voices

Conversations about cyber security professionalisation tend to be dominated by a familiar cast of stakeholders: government departments and agencies, large employers, certification bodies, academic institutions, and a smattering of non-governmental organisations. These all have important roles to play, particularly in enacting some of the proposals suggested herein, but they do not represent the complete cyber security community. Any discussion about the community ought to have appropriate representation from a range of voices to ensure a diversity of views and experiences are taken into account when developing the cyber security profession. Two stakeholders can be particularly identified as requiring more effort to integrate into the conversation. First, there is a potentially untapped pool of talent in what might be called uncertified excellence: individuals with relevant cyber security knowledge, skills, and possibly experience, that have not been recognised through certification or other accreditation (for example university degrees). These people can be aspiring or existing cyber security professionals, but their voice is underrepresented in discussions shaping their own profession. Second, small and medium enterprises

(SMEs) – both cyber security SMEs and SMEs in other sectors. Cyber security SMEs need cyber security professionals to deliver their core business services or products. Other SMEs have a more complicated need for cyber security skills, often lacking resources for dedicated personnel and instead needing people who can perform cyber security roles as add-ons to other roles. The cyber security profession should cater to these needs, and therefore have these voices adequately represented in the development of the profession.

To ensure the voices of uncertified excellence and SMEs have opportunities to be involved in professionalisation discussions, it is possible to extend efforts towards interoperability. By emphasising a skills-first approach in interoperability, rather than an accreditations-first or experience-first approach, those people who have skills but not accreditations or experience can be foregrounded. Similarly, a skills-first approach would aid SMEs, particularly non-cyber security SMEs, in accessing the skills they need for their specific requirements. A skills-first approach would provide a focal point for making frameworks and standards interoperable.

Further research

While some of the issues covered above are well understood and grounded in a solid evidence base, others remain less illuminated with little more than anecdotal evidence in support. This suggests a requirement for further research to build a broader and deeper selection of data which can be used to make international comparisons and inform decisions about cyber security professionalisation. The Cyber Security Skills in the UK Labour Market report published annually by the UK government remains best in class for this type of research. While some efforts have been made to emulate it in other countries, the international community would greatly benefit from increased proliferation of this research to build a common understanding of cyber security workforce challenges. Such research, when conducted using comparable methodologies, would also be a fundamental part of creating a shared glossary of terms as well as tracking progress in cyber security professionalisation. In addition, there is need for a new piece of research investigating the future cyber security workforce, with a focus on quantifying the workforce at various time horizons. This would help ensure supply (from education and training systems) today can be matched to future demand. It could also be used to identify cyber security roles, if any, that are likely to be eliminated by new technologies. A core principle to bear in mind during any research into skills is that there is a difference between individual perception of needs

and organisational perception of needs. It is therefore crucial to have a diverse selection of voices represented in research to collect a broad range of views.

Next steps

There is great value in international dialogue to advance cyber security professionalisation. Countries can learn a lot from each other, with government, industry, academia, and accreditation providers all serving important roles. While some bilateral and multilateral efforts are already underway, a timely opportunity exists to build an international community to take the six core recommendations herein forward

- Creating a shared glossary
- Understanding similarities and differences in countries' approaches
- Setting a common baseline for quality
- Making national frameworks and standards interoperable
- Establishing an adoption plan for both private and public sectors
- Promoting efforts and tracking progress

The cyber security profession is a force for good; the international community can embed and enhance its potential.

Andreas Haggmann

Wilton Park | November 2024

Wilton Park reports are brief summaries of the main points and conclusions of a conference. The reports reflect rapporteurs' personal interpretations of the proceedings. As such they do not constitute any institutional policy of Wilton Park nor do they necessarily represent the views of the rapporteur. Wilton Park reports and any recommendations contained therein are for participants and are not a statement of policy for Wilton Park, the Foreign, Commonwealth and Development Office (FCDO) or His Majesty's Government.

Should you wish to read other Wilton Park reports, or participate in upcoming Wilton Park events, please consult our website www.wiltonpark.org.uk.

To receive our monthly bulletin and latest updates, please subscribe to www.wiltonpark.org.uk/newsletter

Wilton Park is a discreet think-space designed for experts and policy-makers to engage in genuine dialogue with a network of diverse voices, in order to address the most pressing challenges of our time.

enquiries@wiltonpark.org.uk

Switchboard: +44 (0)1903 815020

Wilton Park, Wiston House, Steyning,
West Sussex, BN44 3DZ, United Kingdom

wiltonpark.org.uk