Addressing cyber security skills: the spectrum, not the silo


Steven Furnell


Matt Bishop

Steven Furnell, Centre for Security, Communications and Network Research, University of Plymouth, UK and Matt Bishop, Department of Computer Science, University of California at Davis, US

With cyber security gaining ever-greater recognition as a key concern in today's organisations, there is an accompanying appreciation that specialist skills are required to support it. However, this has created challenges for employers in recruiting the associated talent, not least because skilled staff are in short supply.

Indeed, there is ample evidence of a skills shortage, as illustrated by recent industry studies:

- EY's 'Global Information Security Survey 2018-19' suggested that 30% of organisations were struggling with skills shortages, placing the issue ahead of budgetary constraints, cited by 25%.[1]
- More than half (53%) of IT professionals surveyed by Enterprise Strategy Group cited a 'problematic shortage' of cyber security skills as their top issue.[2]
- (ISC)[2] found that 65% of organisations reported a skills shortage, with 51% considering that their organisation was at moderate or extreme risk as a result. The same study suggested a global skills gap of 4.07 million.[3]

Moreover, the growing demand for additional skills looks unlikely to abate. For instance, a June 2019 study from Burning Glass indicated that 'cyber security knowledge' was the fastest-growing skill in relation to computer support and networking, with a five-year projected growth of 120%. Additionally, the related issue of threat intelligence and analysis was next in the list, with 87%.[4]

What it means

Having established that there is a shortage of cyber security skills, it is relevant to understand what this actually means and what we should be looking for. Some view cyber security as a term encompassing what used to be called information security, while others insist it means something distinct. Without getting into the specifics of that debate, it is not surprising that understanding and recognising the knowledge, skills and abilities required to deliver cyber security is a blurry area.

Regardless of how it is defined, it is clear that cyber security as a whole is a multi-faceted discipline, encompassing both technical and non-technical topic areas. The technical topic areas span various issues around system, device and network security, which in turn include a range of underlying mechanisms. Non-technical elements include managerial, human, legal and physical protection perspectives.

Some evidence of the importance of non-technical aspects comes from (ISC)[2]'s 2018 study into hiring and retaining talent.[5] It identifies the following top five skills most commonly used among the 250 cyber professionals that responded: cyber security strategy; cyber security management; user education; risk assessment; and security operations. Non-technical aspects clearly dominate the list, and while the responses were likely skewed by the nature of the more senior level of the respondents (64% were middle management level or higher), this is also part of the point. Technical skills may dominate some of the lower-level cyber roles, but individuals need the broader understanding and skillset in order to progress in their careers.

In practice, however, there is an apparent skew towards the technical perspective, which is unsurprising in a market that is packed with product-based technology solutions. This in itself can represent a risk,

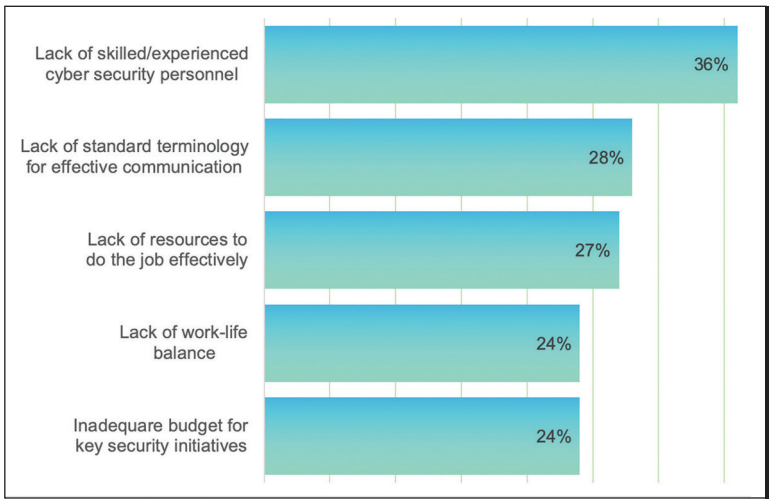

Figure 1: Top job concerns among cyber security professionals. Source: (ISC)[2].

Source	Framework	Description / Coverage
ACM/IEEE/AIS/ IFIP	Cybersecurity Curricula 2017 (CSEC2017)[6]	Produced by the ACM/IEEE/AIS/IFIP Joint Task Force in 2017, the guidelines provide a structure for the cyber security discipline, defining its boundaries and outlining key dimensions of a curricular structure. It identifies eight knowledge areas: data security; software security; component security; connection security; system security; human security; organisational security; societal security.
CIISec	Skills Framework v2.4[7]	The Skills Framework describes the range of competencies expected of information security and information assurance professionals in the effective performance of their roles. It is based on 11 security disciplines: information security governance and management; threat assessment and information risk management; implementing secure systems; assurance, audit, compliance and testing; operational security management; incident management, investigation and digital forensics; data protection, privacy and identity management; business resilience; information security research; management, leadership, business and communications; contributions to the information security profession and professional development.
CyBOK project	Cyber Security Body of Knowledge (CyBOK)[8]	An initiative funded by the UK's National Cyber Security Programme and seeking to codify the foundational and generally recognised knowledge on cyber security. It proposes 19 knowledge areas: risk management & governance; cyber physical systems; law & regulation; physical layer and telecommunications security; human factors; secure software lifecycle; privacy & online rights; operating systems & virtualisation security; adversarial behaviours; malware; network security; security operations & incident management; cryptography; software security; authentication, authorisation & accountability (AAA); web & mobile security; hardware security; distributed systems security; forensics.
(ISC)^2	Common Body of Knowledge (CBK)[9]	The CBK is used as the underlying knowledge base for (ISC)^2's series of professional certifications, including CISSP, SSCP and CCSP. It identifies eight domains: security and risk management; asset security; security architecture and engineering; communications and network security; identity and access management; security assessment and testing; security operations; software development security.
ISO/IEC	27002:2013 – Code of Practice for Information Security Controls[10]	An international standard designed as a reference for organisations to use in selecting common security controls, as well as offering guidance on their use. It is structured around 14 main clauses: information security policies; organisation of information security; human resource security; asset management; access control; cryptography; physical and environmental security; operations security; communications security; systems acquisition, development and maintenance; supplier relationships; information security incident management; information security aspects of business continuity management; compliance.
NIST	National Initiative for Cyber security Education (NICE) Cybersecurity Workforce Framework[11]	The NICE Framework aims to provide a common, consistent lexicon that categorises and describes cyber security jobs, and a reference for describing and sharing information about the knowledge, skills and abilities involved. It is based upon seven categories: analyse; collect and operate; investigate; operate and maintain; oversee and govern; protect and defend; securely provision.
NSA	Centres of Academic Excellence (CAE) Knowledge Units[12]	The Centres of Academic Excellence programme identifies four classes of knowledge unit: fundamental (cyber security foundations; cyber security principles; IT systems components); technical core (basic cryptography; basic networking; basic scripting and programming; network defence; operating systems concepts); non-technical core (cyberthreats; cyber security planning and management; policy, legal, ethics, and compliance; security programme management; security risk analysis); and optional (spanning 56 further units covering both technical and non-technical aspects of security, as well as more general computing and communications topics). The knowledge units are then used within designated specialisations for cyber defence education (CAE-CDE), cyber defence research (CAE-R) and cyber operations (CAE-CO). All designations require the fundamental units to be covered and various percentages and combinations of the others.

Table 1: A summary of the selected cyber security frameworks.

insofar as over-focusing on one part of the picture leaves the potential for vulnerabilities in the other. Moreover, we know that technology does not exist in isolation – it is used by people to support the business. As such, they need to be able to join up, and this is unlikely to happen if we only have the skills in one area. This does not mean that all cyber security staff should be expected to cover all areas, but the organisation as a whole must find a way to do so.

Different views

Although it is readily accepted that cyber security encompasses a variety of underlying topics, there is no definitive list of the issues or their associated structure. There are, however, a number of recognised frameworks that can be regarded as reference points for the discipline and it is relevant to examine the extent to which the technical and non-technical perspectives are represented within them. With this in mind, Table 1 looks at a selection of key frameworks, with origins spanning the academic, industry and professional communities.

Looking at the coverage within each framework, it is clear that they are taking rather different views of how cyber security breaks down at the topic level, with some notable differences in the extent to which they focus upon the technical and

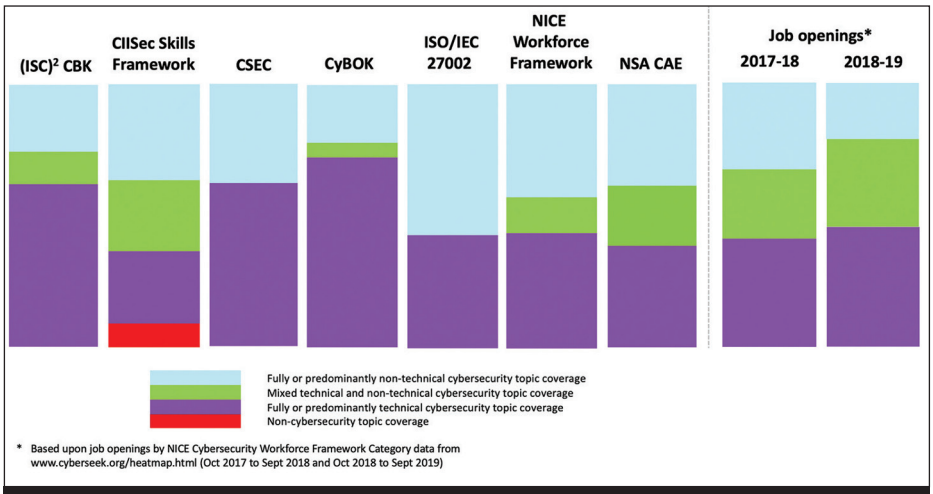

Figure 2: Topic coverage within alternative cyber security frameworks.

non-technical aspects of the discipline. Figure 2 groups the underlying units (domains, groups or knowledge areas) into different categories according to their predominant coverage as assessed by the authors. Presented in this format, it is easy to see that there are considerable differences in the approaches, with the CyBOK and ISO/IEC 27002 cases offering the most obvious contrast in terms of how they appear to position their coverage. The CIISec Skills Framework distinguishes itself by being the only framework with a topic area that was classified as offering non-cyber security coverage (this being the management, leadership, business and communications area, which still remains relevant as it covers soft skills, which are much needed within cyber security).

Another point to note is that the entry for the NSA's Centres of Academic Excellence only considers the topic coverage among the fundamental and core knowledge units (as listing all of the optional units would give a skewed impression, given the overall volume of them and the fact that many have a non-security focus). The columns relating to job openings are based upon vacancy data that had originally been mapped to the NICE Workforce Framework, and was then further mapped to the broader categorisations used in the chart. As such it is provided for the purposes of general comparison rather than a specific assessment of the market for this study.

Point of reference

Ultimately, the frameworks partition the subject rather differently and it is easy to appreciate that the notion of cyber security can end up looking rather different depending upon which is used as the point of reference. This becomes significant when one then considers the different roles that they may have in shaping the cyber security skills base.

Indeed, some of them feed directly into academic qualifications and professional certifications, which in turn help to inform (and later denote) those individuals forming part of our cyber security workforce. In this context, some frameworks directly define the content that gets covered (eg, the (ISC)^2 CBK underpins its related certifications, such as CISSP and SSCP, while the CSEC is intended to directly guide undergraduate academic curricula), whereas others will have a role in doing so indirectly (eg, the ability for providers to map their course content against CyBOK or the NSA CAE criteria in order to show what aspects they are focusing upon).

Cyber security practitioners raised on different frameworks could clearly end up with dramatically different perceptions of what they should be concerned with and responsible for. The question for organisations is whether they have all the necessary bases covered.

Moreover, the coverage variation between the security frameworks is only part of the story. The potential to emphasise different perspectives on cyber security also cascades into the qualifications and certifications that people can pursue and then present as evidence of their capability.

Looking at academic qualifications, there can be a dramatic difference in what gets covered, even when the degree programmes share exactly the same name. So, while one can easily find multiple degrees that are all titled 'MSc cyber security', the actual module coverage can differ significantly between them – to the extent that some programmes can have entirely technical coverage, while others can readily be found that include a significant proportion of non-cyber modules.[13] Meanwhile, the situation with industry and professional certifications is different, insofar as many of them take a more topic-specialised stance in the first place. Nonetheless, it is still important to understand what aspects of security they relate to, and thereby what being a holder of the certification implies that someone can understand and do.

Industry imbalance?

While we continue to face a shortage of practitioners, there is ironically no shortage of the qualifications and certifications that they may hold. However, navigating through the myriad options can be a significant challenge, and this is further amplified when one realises that – as with the above frameworks – many of them regard and address cyber security in fundamentally different ways.

If we look at the marketplace of cyber security certifications, the industry is awash with qualification options. A 2017 assessment by Tittel et al revealed over 100 on offer from various providers[14] Some of these are more mainstream than others (in terms of both recognition and coverage), whereas some focus upon very specific aspects or technologies. Nonetheless, all of them exist as options that cyber security practitioners could

conceivably be holding and promoting in order to demonstrate their credibility.

So, it is essential for those seeking to hire or employ staff to realise that the skills they represent are actually different. In short, you need to know what skills you are looking for and what certifications are likely to embody them. However, as observed in a previous paper, it is all too easy to find job advertisements that seem to imply that different certifications are essentially interchangeable, accepting applications from a Security+ holder as readily as they would a CISSP or a CISA, when in reality the certifications denote something considerably different in terms of topic and experience.[15]

The fact that all certifications are not equal is also apparent in other ways. Figure 3 illustrates the relative supply and demand of some of the more well-known options, based upon data from Cyberseek.org.[16] Looking at the resulting chart, (ISC)²'s CISSP certification is, unsurprisingly, the certification with the highest level of overall demand. Indeed, looking at many cyber security job advertisements, CISSP seems to have become the certification that employers most often ask for – although this may be due to its brand identity and recognition rather than employers specifically matching their needs to what certificate holder would offer them, or perhaps because it is seen as a useful proxy for signifying that someone has a credible level of experience as a practitioner.

However, the certification in most ready supply is the more entry-level CompTIA Security+. This is very likely due to the relative ease of achieving it, because it does not depend upon prior experience (whereas this is, of course, exactly what many employers will actually be seeking, which in turn accounts for the relative lack of demand). Looking to the remaining items, there is a notable concentration of items with a lower number of certification holders.

Setting aside the newer and more specialised CIPP certification, for which supply and demand are consequently lower at present, this leaves three items for which

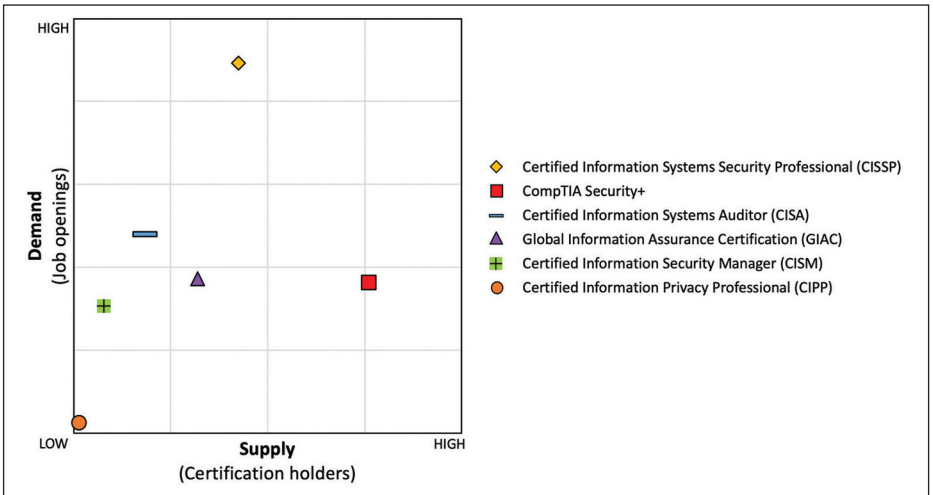

Figure 3: Supply and demand for different professional certifications.

demand appears relatively clear but where supply is lagging. Of these, there is a notable under-supply of the certifications focusing on non-technical aspects, namely CISA and CISM. Indeed, while the ratio of certification holders to related job openings for Security+ is 3.33:1, for CISA and CISM it is 0.60:1 and 0.40:1 respectively. Meanwhile, in contrast to the other entries, the GIAC item represents a certification series rather than a single offering (spanning almost 40 distinct certifications, across seven categories), with the underlying certifications spanning both technical and non-technical aspects of cyber security (see www.giac.org/certifications/categories for a full list).

The shortage of certification holders for CISA and CISM is worth further consideration. In part, it is likely to be a natural consequence of these certifications requiring candidates to have several years of relevant work experience. However, the same holds true for CISSP, and although there is an under-supply issue there as well, it is less dramatic (at 0.754:1). So, there appears to be something else happening in the cases of CISA and CISM, and it seems reasonable to hypothesise that fewer people are being channelled towards these aspects of cyber security in the first place. This in turn may relate back to how they learned about the topic and how it was presented to them. If the breadth of the topic is not getting the appropriate visibility, then it will add to the challenge of getting sufficient people engaged with it.

What we really want

The discussion to this point helps to emphasise that dealing with cyber security staffing needs is not just a question of hiring someone with a particular badge – we need to see that badge in the context of our needs. What does it add to the portfolio of skills that we are trying to ensure across our cyber-related roles?

Figure 4 represents a view of the relationship between certifications and other aspects that will help to define the basis for a cyber security career. The knowledge, skills and competencies are what we actually want. The certifications are a representation of those in a form designed to enable others to make a preliminary assessment of the holder's knowledge, skills and competencies. Therefore, a certification means that, at some point in time, the person had the knowledge, skills and competencies commensurate with that certification, and could pass the requisite tests. Similarly, roles (jobs) require people with certain knowledge, skills and capabilities. If the (prospective) employee has experience in the tasks the role encompasses and the employer knows it, then the representation of those skills (the certifications) are typically ignored, whereas if the employer does not know the experience of the (prospective) employee, the certifications will enlighten him or her to some degree. So the certifications become a proxy for representing knowledge, skills

and competencies. They will not always be an essential element in order to perform a given role, and hence the lines here are dotted to signify an optional relationship.

Interestingly, employers often do not know what they need – they only think they know. Many will end up relying upon the much sought-after – but potentially ill-defined – commodity of 'experience', with the implicit assumption that if someone has already been doing the job elsewhere, then they can do it for us as well. This other aspect of experience serves the employer, because the employee can bring knowledge from previous jobs to advise the employer what he needs. It is obviously good as a means of ensuring that someone has practical experience and not just theoretical knowledge, but it does not remove the need to know what you are looking for.

Fitting the picture

One might also ask where experience fits into the picture. One way of viewing it would be as an attribute within skills. Another option would be for it to sit in the box alongside certifications. However, experience is temporal by definition – for example, the Merriam-Webster dictionary defines it as "practical knowledge, skill, or practice derived from direct observation of or participation in events or in a particular activity", combined with the length of such participation.

To incorporate it into this model we add a time attribute to each of the nodes. As the person gains better or new skills, knowledge, and competencies, he or she may add certifications. Equally, as they focus on specific roles, their certifications may lapse. Similarly, although job titles may be static, the tasks associated with those titles also change.

What is clearly needed is a greater sense of clarity and a means to join up the elements in Figure 4 in a way that helps to define cyber security not only in terms of topics, skills and qualifications, but in a meaningful structure for careers and professional progression. Fortunately, there are already contributions in this direction. In the US, the NIST NICE Workforce Framework explicitly positions itself as "a fundamental reference resource for describing and sharing information about cyber security work and the knowledge, skills and abilities (KSAs) needed to complete tasks that can strengthen the cyber security posture of an organisation". It lists the KSAs that specific work roles require and so serves as a guide for companies enhancing their cyber security groups. A similar contribution is made by the CIISec Roles Framework, which takes 11 common roles (including CISO, pen tester, security architect, and threat analyst) and maps them to the primary and secondary skills areas that are considered relevant (as well as the qualifications and experience that one might expect to see).[17]

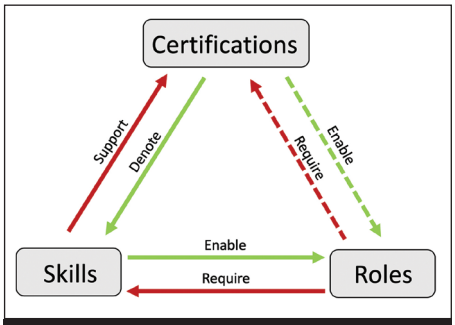

Figure 4: Relationships between certifications, skills and roles.

Adding to the above, the emerging UK Cyber Security Council has a specific workstream on the theme of qualifications, with the stated objective of defining "a clear route through the profession incorporating qualifications, certifications and associated policies".[18] Within this is a clear recognition that these qualifications are intended as elements to help people develop an associated career. As such, it is clear that necessary elements are emerging and receiving further attention. However, there is still a way to go before they are used in practice as the de facto points of reference for employers and the industry at large.

Conclusions

Regardless of the specific topic balance in the individual cases, the various cyber security frameworks clearly demonstrate that the discipline covers a range of technical and non-technical issues. As such, it is important to recognise the breadth of skills needed and ensure that they are in some way covered. The natural way to do this is to recruit talent with suitable certifications or qualifications, but for this to work we need to understand what they cover and whether it matches what we need.

If we take a siloed approach to cyber security skills, then we risk severely limiting the protection that can be achieved. Equally, in seeking a solution, it is not just about recognising that a spectrum of skills is required – we also need to get them to work together in an effective manner.

About the authors

Professor Steven Furnell is a professor of information security and leads the Centre for Security, Communications & Network Research at the University of Plymouth. He is also an adjunct professor with Edith Cowan University in Western Australia and an honorary professor with Nelson Mandela University in South Africa. His research interests include usability of security and privacy, security management and culture, and technologies for user authentication and intrusion detection. He has authored over 320 papers in refereed international journals and conference proceedings, as well as books including Cybercrime: Vandalizing the Information Society *and* Computer Insecurity: Risking the System. *Furnell is the current chair of Technical Committee 11 (security and privacy) within the International Federation for Information Processing, and a member of related working groups on security management, security education and human aspects of security. He is also a board member of the Chartered Institute of Information Security and chairs the academic partnership committee and southwest branch.*

Matt Bishop is a professor in the Department of Computer Science at the University of California at Davis, and a co-director of the Computer Security Laboratory

there. His research interests include vulnerabilities analysis, data sanitisation, the insider problem, elections and electronic voting and tallying systems, assurance and cyber security education. He has been active in cyber security education; he co-chaired the ACM/IEEE Computer Society/AIS SIGSEC/IFIP WG 11.8 Joint Task Force that developed the Cybersecurity Curricula Guidelines (CSEC2017), and has worked on methods to improve the state of programming and teaching programming. His textbook, Computer Security: Art and Science, is now in its second edition and is used in many undergraduate and graduate cyber security programmes.

References

1. 'Is cyber security about more than protection?' EY Global Information Security Survey 2018-19. EYG no. 011483-18Gbl.
2. Oltsik, J. 'The cybersecurity skills shortage is getting worse'. ESG Blogs, 10 Jan 2019. Accessed Jan 2020. www.esg-global.com/blog/the-cybersecurity-skills-shortage-is-getting-worse.
3. 'Strategies for building and growing strong cyber security teams: (ISC)^2 Cybersecurity Workforce Study, 2019. Accessed Jan 2020. www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx.
4. Nania, J; Bonella, H; Restuccia, D; Taska, B. 'No Longer Optional: Employer Demand for Digital Skills'. Burning Glass Technologies and Department for Digital, Culture, Media and Sport, June 2019. Accessed Jan 2020. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/807830/No_Longer_Optional_Employer_Demand_for_Digital_Skills.pdf.
5. 'Hiring and retaining top cyber security talent: What employers need to know about cyber security jobseekers in 2018'. (ISC)^2, 2018. Accessed Jan 2020. www.isc2.org/-/media/Files/Research/ISC2-Hiring-and-Retaining-Top-Cybersecurity-Talent.ashx.
6. 'Cybersecurity Curricula 2017 – Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity'. CSEC2017 Joint Task Force, 2017. Version 1.0 Report 31 December 2017. Association for Computing Machinery (ACM), IEEE Computer Society (IEEE-CS), Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC) and International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8). Accessed Jan 2020. https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf.
7. 'CIISec Skills Framework'. Version 2.4, Chartered Institute of Information Security, November 2019. Accessed Jan 2020. www.ciisec.org/CIISEC/Resources/Capability_Methodology/Skills_Framework/CIISEC/Resources/Skills_Framework.aspx.
8. Rashid, A; Chivers, H; Danezis, G; Lupu, E; Martin, A. 'The Cyber Security Body of Knowledge'. Version 1.0, 31 Oct 2019. Accessed Jan 2020. www.cybok.org/media/downloads/cybok_version_1.0.pdf.
9. 'The (ISC)² CBK'. (ISC)². Accessed Jan 2020. www.isc2.org/Certifications/CBK.
10. 'Information technology – Security techniques – Code of practice for information security controls. International Standard ISO/IEC 27002. Second edition 2013-10-01'. International Organisation for Standardization and International Electrotechnical Commission (ISO/IEC), 2013.
11. Newhouse, B; Keith, S; Scriber, B; Witte, G. 'National Initiative for Cybersecurity Education (NICE), Cybersecurity Workforce Framework. NIST Special Publication 800-181'. NIST, Aug 2017. Accessed Jan 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.
12. 'CAE-CD 2020 Knowledge Units. CAE Requirements and Resources'. National Security Agency (NSA), 2019. Accessed Jan 2020. www.iad.gov/NIETP/documents/Requirements/CAE-CD_2020_Knowledge_Units.pdf.
13. Furnell, S; Bishop, M. 'Education for the multi-faith community of cyber security'. To appear in proceedings of the 13th World Conference on Information Security Education (WISE13), Maribor, Slovenia, 26-28 May 2020.
14. Tittel, E; Lemons, M; Kyle, M. 'Information security certifications: Introductory level'. TechTarget, Dec 2017. Accessed Jan 2020. http://searchsecurity.techtarget.com/tip/SearchSecuritycom-guide-to-information-security-certifications.
15. Furnell, S; Fischer, P; Finch, A. 'Can't get the staff? The growing need for cyber security skills'. Computer Fraud & Security, Feb 2017, pp.5-10. Accessed Jan 2020. www.sciencedirect.com/science/article/pii/S1361372317300131.
16. 'Cyber security supply/demand heat map'. Cyber Seek, 2018. Accessed Jan 2020. www.cyberseek.org/heatmap.html.
17. 'CIISec Roles Framework, Version 0.3'. Charted Institute of Information Security, Nov 2019. Accessed Jan 2020. www.ciisec.org/CIISEC/Resources/Capability_Methodology/Roles_Framework/CIISEC/Resources/Roles_Framework.aspx.
18. 'Workstream 6: Qualifications'. UK Cyber Security Council Formation Project, The Institution of Engineering and Technology (IET), 2019. www.theiet.org/impact-society/uk-cyber-security-council-formation-project/qualifications/.