



**Curry, J. and Bird, D.A. (2018) 'A case for using blended learning and development techniques to aid the delivery of a UK cybersecurity core body of knowledge', *International Journal of Systems and Software Security and Protection*, 9 (2), pp. 28-45.**

"Through IGI Global's Fair Use Policy, authors may post the final typeset PDF of their chapter or article on the author or editor's secure personal website and/or their university repository site." – details [here](#).

To access the final work on the publisher's site go to <http://dx.doi.org/10.4018/IJSSSP.2018040103>

## ResearchSPAce

<http://researchspace.bathspa.ac.uk/>

This version is made available in accordance with publisher policies.  
Please cite only the published version using the reference above.

Your access and use of this document is based on your acceptance of the ResearchSPAce Metadata and Data Policies, as well as applicable law:-

<https://researchspace.bathspa.ac.uk/policies.html>

Unless you accept the terms of these Policies in full, you do not have permission to download this document.


This cover sheet may not be removed from the document.

Please scroll down to view the document.

# A Case for Using Blended Learning and Development Techniques to Aid the Delivery of a UK Cybersecurity Core Body of Knowledge

David A Bird, Learning and Performance Institute, Coventry, UK

John Curry, Bath Spa University, Bath, UK

 <https://orcid.org/0000-0003-2872-0678>

## ABSTRACT

This article explores the UK's current approach in addressing the cybersecurity skills gap championed by the National Cyber Security Strategy. There have been progressive and elaborate steps taken in the UK toward professionalization of the cybersecurity field. However, cybersecurity knowledge has been labelled as inconsistent when a cybersecurity Chartered status is being proposed. The objective of this analysis was to apply an academic lens over the UK's voyage towards the establishment of a cybersecurity profession. It has been an ambitious but complex endeavor that at times has had alterations of course. Learning from this experience, a blended learning and development approach is now recommended underpinned by an overarching core knowledge framework. Such a framework could join up the existing silos of learning and development activities to benefit from, and build upon, a coherent core knowledge-base for the community. It is argued that this will provide a more satisfactory outcome to enhance the UK's cybersecurity capability on the road to a cybersecurity profession.

## KEYWORDS

Blended Learning Approach, Core Knowledge Framework, Cybersecurity, Learning and Development, Strategies

## 1. INTRODUCTION

In 2011, the United Kingdom (UK) Government set out their stool by predicting the need to increase cybersecurity skills and expertise in line with their Cyber Security Strategy. It was also decreed that education and training providers should heed this prediction. The main aim then was to counter the effects of cyber-crime, which required specialist training in order to meet an increased skills demand (Cabinet Office, 2011). In 2013, the Harvard Business review stated that education was a catalyst, and enabler, for cybersecurity and called upon academic institutions to share cybersecurity best practices and curricula (Viveros, 2013).

The comprehensive International Information Systems Security Certification Consortium ((ISC)<sup>2</sup>) survey of 2015 stated that 63% of private sector organizations did not have enough cybersecurity

DOI: 10.4018/IJSSSP.2018040103

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

staff in the UK (Grout, 2015). In the same year the Chancellor laid out the cyber-crime threats to the UK economy (Osborne, 2015). He labored the point that cybersecurity should be embedded at every stage of the education and training process, so the next generation will be able to keep Britain safe in cyberspace. By the next iteration of the Cyber Security Strategy in 2016, it was stated that there were still insufficient skills in cybersecurity and that the public lacked cyber awareness. The UK Government subsequently set their intention for collaboration in training and education across the target audience in the public and private sectors (Cabinet Office, 2016). This was a part of the continuing agenda taken by UK Government to make Britain the safest place in cyberspace championed by the Department for Digital, Culture, Media and Sport (DCMS) (2017) and the National Cyber Security Center (NCSC) which is a part of the Government Communications Headquarters (GCHQ). A number of approaches to enthuse adolescents were spawned and aimed at refocusing of attitudes leading to a cybersecurity curriculum (Williams, 2017).

There is a myriad of certifications categorized by the Institute of Information Security Professionals (IISP) ranging from vendor-based, those aimed at role competencies, broad certifications and those provided by academia (Finch & Furnell, 2018). However, there are advantages and disadvantages with professionalization. From a USA perspective, Schneier (2013) has discussed openly that popular certifications used as a form of entry into cybersecurity run the risk of becoming obsolete; and need to be maintained using Continuous Professional Development (CPD). Interestingly, Nepal (2018) has stated that in Australia cybersecurity tools have not reduced the demand on cybersecurity experts, but actually increased demand for more cybersecurity specialists. In tandem, the cybersecurity skills shortage in the UK increased to 66% by 2017 (Cox, 2017). The 2018 edition of Information Systems Audit and Control Association (ISACA) 'State of Cybersecurity' report stated that of the 60% of organizations who had open jobs in cybersecurity, 54% of positions took over three months to fill (GoCertify, 2018); it was suggested that the skills gap was actually widening (ISACA, 2018). Consequently, demand for expertise and skills is driving up cybersecurity salaries in the UK (McDonald, 2018) and making them comparative to more established and recognized professions.

Additionally, there have been endeavors to increase cybersecurity awareness in organizations (Palmer, 2016) and the wider populace of the UK; this follows a similar agenda to the USA (Morgan, 2017). However, awareness should only be the start of making people mindful about the cybersecurity risks (Beyer et al., 2015). There are other diverse and relevant skillsets within the Information Technology (IT) industry such as system designers and developers along with system managers and system administrators who are also important in cybersecurity. All these roles require better cybersecurity awareness and the right culture to ensure that security is an important criterion in the development, implementation and maintenance of new systems. According to a survey by Harvey Nash and PGI (2016) the creation of a security-aware culture has been the most critical yet lacking action in the past.

However, to fill the cybersecurity skills shortage there has been a concerted push aimed at practitioners working in the cybersecurity discipline across many specialist fields – ranging from risk management consultants to penetration testers to security analysts in security operations centers. Existing learning options and methods for establishing qualified practitioners in cybersecurity have been developed in isolation of each other and as a result are fragmented. While they contribute to a career outcome, the disparate development and delivery techniques are not joined up. It is surmised that a study is needed to qualify the cybersecurity foundational knowledge and determine the best relevant learning options to achieve a holistic approach. That is, which mix of online learning, lectures, vocational and practical applications and competition options could fill the skills gaps in a more efficient manner; and how can they can be integrated into schools, academia and certifications in order to strengthen a defined career pathway?

In principle, this errs towards a reason to implement a mixed-mode learning approach of blended-learning techniques and experiences (Great Schools Partnership, 2014). Traditionally used across training and education, blended learning is normally associated with learning-at-a-distance and on campus lectures (Pop, 2018). However, in this context blended learning and development is

aimed at the next dimension to enable a hybrid learning-delivery model (Great Schools Partnership, 2014) that crosses the cybersecurity role divide in support of the overall agenda championed by the Cyber Security Strategy.

## 2. BACKGROUND

There are a number of diverse training, education and professionalization agendas concurrently underway in the UK to fill the cybersecurity skills gap – some are already established such as certifications and others are evolving such as professionalization. In 2015, the report entitled the ‘State of Cybersecurity: Implications for 2016’ stated that nearly 65% of applicants applying for entry-level cybersecurity jobs lacked the requisite skills to perform the job roles that they were seeking (ISACA, 2015); by 2017 37% of respondents declared that fewer than one in four had the qualifications needed to keep their organization secure (ISACA, 2017). Within the report skills development statistics were attributed to the following areas (from the highest to the lowest): (a) 86% was based around on-the-job training, (b) 63% through training and certifications, (c) 38% through certifications around performance-based assessment, (d) 27% through third-party training providers, (e) 16% through formal education, and (f) 5% through competitions. In addition, the recent UK Cybersecurity Breaches Survey indicates that cybersecurity training statistics in business are: (a) 76% of training is for managers, (b) 30% for IT staff, (c) 26% for cybersecurity specialists and 25% for all other staff (DCMS, 2018); denoting that the specialists purportedly filling a key skills gap are trained no more frequently than other staff members.

The next section provides a case-study that articulates the UK’s approach to addressing the cybersecurity skills gap. The chronology of the disparate training, education and professionalization efforts are ordered in line with the previous arguments from the paragraph above.

### 2.1. Staff Training

Training, education and awareness has been considered as part of the legacy UK Government Information Assurance (IA) Maturity Model (IAMM); it was developed by the former Communications Electronic Support Group (CESG) (CESG, 2015) that has now become the NCSC. During its time the IAMM was regarded as best practice for public sector organizations to aspire to. It was also a statement on the ability of any adoptive organization to implement an appropriate information security regime (Office of National Statistics, 2011). However, over time the IAMM became dated and its relevance blurred, so from 2018 it is no longer formally supported (Anne W, 2018a). From a public awareness perspective, in 2016 a Massive Open Online Course was designed and implemented by academia and promoted by the former UK Government’s department called Business, Innovation and Skills, now known as DCMS. It has been awarded Certified Training (CT) status by GCHQ and is recognized by bodies like the IISP for its content adequacy (IA Advisory Council, 2016; Open University, 2018).

### 2.2. Certifications

#### 2.2.1. Traditional

Information security certifications have been the longest reigning entry point for practitioners to become qualified in the cybersecurity domain. Various popular brands emanating from the USA tend to follow in popularity terms within the UK. Four certifications are prominent on both sides of the Atlantic (DeGroat, 2018; Tittel & Lindros, 2018; Afifi-Sabit, 2018; MashableUK, 2018):

- Certified Ethical Hacker
- (ISC)<sup>2</sup> Certified Information Security Systems Professional (CISSP)
- CompTIA Security +
- Certified Information Security Manager

These certifications target penetration testers, IA practitioners and managers and currently fall under the generalist category of certifications. There are other UK exams provided by the British Computer Society (BCS) (2018), the Centre for Research and Evidence on Security Threats (CREST) (CREST, 2018a) and courses that are endorsed by the IISP (IISP, 2018). The CREST accreditation and certification body not only provides offerings in the cyber defense area but also in the penetration testing field. The SysAdmin, Audit, Network and Security (SANS) Institute provides a plethora of role-based certifications and is well known for its Global IA Certification. Within the computer network defense realm, SANS certifications are highly prized in the USA and in the UK. Additionally, SANS is an accredited partner of UK Government organizations and offers training academy options (SANS, 2018).

Under the current Cyber Security Strategy, the NCSC has implemented a CT approach that recognizes core training of non-academic course materials and the training delivery from training providers. The logic behind this approach is that the certification of training providers validates the quality of the training as being of an adequate standard (NCSC, 2018a; NCSC, 2018b). These courses can lead to an exam component of popular brands of exam-based certifications previously listed.

### **2.2.2. Competency-Based**

Competency-based certifications have become popular in the UK. Offensive Security Certified Professional (OSCP) (Wikipedia, 2018) is popular for the penetration testing (Pentest) discipline in the USA and has become so in the UK as well. For Pentest practitioners operating in the UK public sector, additional qualifications centered around CESG's CHECK initiative are required. CHECK Team Member and CHECK Team Leader qualifications are available through the Tigerscheme (Tigerscheme, 2018) and CREST (CREST, 2018b) as a comparable qualification to the CHECK Team Member. In addition, through a set of eligibility criteria, CREST offers CREST Registered Tester equivalency for practitioners holding the OSCP certification not only in Australia and New Zealand, but also in the USA (CREST Australia, 2017).

For IA consultants working in the public sector, the UK Government originally levied a requirement for the Infosec Training Paths and Competencies certification. Subsequently, the method of proving demonstrable competencies changed to the Cybersecurity Certified Professional (CCP) scheme (CESG, 2016) that was founded in 2013 (Stevenson, 2013). The CCP scheme standard was originally developed by CESG and is underpinned by the IISP Skills Framework (MacWillson, 2017); a framework that had been corroborated with public sector representatives, academia and industry security leaders (Kleinman, 2018). The CCP scheme is presently administered on behalf of NCSC by three selected Certifying Bodies. The scheme is defined by different role types and various grades within those roles, which was purported to have rectified a criticism of the fore-runner – the CESG Listed Advisor Scheme (CLAS). CLAS was established in 1999 and had originally been proposed as a one-size-fits-all risk assessment and management scheme to support government departments and agencies adopt centralized government focused networks (Bada et al., 2016).

## **2.3. Professionalization**

### **2.3.1. Government Orientated**

The UK Pentest market for the public sector was standardized firstly under the CHECK scheme (NCSC, 2017a) and the status is attributed to a particular company who has reached the threshold number of qualified Pentest staff. It has been so successful that this approach has been heralded as a good example of a professionalization scheme (Knowles et al., 2016). Originally IA consultancy in the public sector was focused around the CLAS membership (Bada et al., 2016). Over time CLAS had grown beyond its original remit and consultants diversified into many different IA skill camps – not just spanning risk assessment, but also including IA Architecture, Auditor and Accreditor roles too. Subsequently, after a period of consultation, CLAS was dissolved in 2015 in favor of the Certified Cyber Security

Consultancy format (Milligan & Rajab, 2015) following a similar approach to the CHECK scheme; again, attributing the status to a company and not any one individual (NCSC, 2016). To be a part of the certified consultancy scheme at least one head consultant must be appointed who has to hold a recognized certification or qualification type (NCSC, 2018b) and be interviewed by NCSC.

### **2.3.2. Community Related**

In the past few years there has been a desire to introduce a cybersecurity Chartered status (Dallaway, 2017; Finch et al., 2018). It was initially thought that this could be conveyed through a chartered institution, but a recent consultation headed by DCMS is veering towards an independent body to ensure that standardization occurs (DCMS, 2018; Chris E, 2018). The UK Government approach is erring towards an independent Cyber Security Council that could act as an umbrella organization of existing professional bodies (Chris E, 2018), similar in function to the UK's Engineering Council and it could ensure that professionalization will follow against a centralized Cyber Security Body of Knowledge (CyBOK). CyBOK itself has been developed as part of the National Cyber Security Program, and advocated as a body of knowledge to distill knowledge orientated around specialisms – these are currently being ratified one-by-one (Rashid et al., 2018).

### **2.3.3. Professional Bodies**

Simultaneously, some of the UK's Chartered professional bodies such as the British Computer Society, The Security Institute, and the Institution of Engineering Technology have combined with other professional bodies to jointly take the initiative on influencing the direction of the cybersecurity profession. These bodies, with other collaborating organizations, have formed the Cyber Security Alliance that also includes the Institute of Analysts and Programmers, the Chartered Institute of Machinery and Control, CREST and (ISC)<sup>2</sup> (CREST, 2018c). The remit of the Alliance is to benchmark shared standards for excellence, skills and capabilities, developing a pipeline of expertise to advise and inform national policy and contribute towards the cybersecurity profession. It is sensible and crucial that the wider community is engaged to establish, develop and recognize additional cybersecurity skills in a consistent and impartial manner.

### **2.3.4. Skills Diversification**

Similarly to the US, the UK has recognized that other skill diversities should be included in the cybersecurity fraternity (Oesch, 2018). The cybersecurity community has been keen to differentiate itself as being gender neutral by encouraging more women into this developing profession (Thomas, 2018). There has also been a concerted effort to promote cybersecurity as an option for reskilling or enhancing the skills of military veterans (Nicholls, 2018). Acceptance of disparate skills into the cybersecurity community is now being actively encouraged and other skills groups are now also being represented (Jones & O'Neill, 2017).

## **2.4. Schools and Higher Education**

There are increasing opportunities in the cybersecurity industry for the younger generation of all genders. The introduction of a cybersecurity curriculum is a positive step for children and adolescents. In pre-university education a new technical version of the Advanced Level qualification has been introduced called a T-Level (Ryan, 2018); this follows the success of an Advanced Subsidiary Level equivalent course which is a pre-cursor to the higher T-Level and was developed as an Extended Project Qualification in cybersecurity (The Engineer, 2016). The UK Government's CyberFirst three-year bursary scheme is aimed at Science, Technology, Engineering and Mathematics (STEM) undergraduate students (TheBigChoice.com, 2018). STEM education is being used to fill the skills gap spanning the next 20 years. STEM follows on from the USA STEM initiative (US Department of Education, 2018) to encourage students into shortage area categories. CyberFirst followed as a

degree apprenticeship and has the aim of kick-starting careers in cybersecurity reinforced by work experience placements (Murphy, 2017).

## 2.5. Academia

There is a plethora of universities in all corners of the UK offering courses that contribute to named cybersecurity degrees. In order to distinguish excellence and nurture growth of the UK's cybersecurity capability, the NCSC has introduced their university degree certification scheme that offers a wide selection of career options and topics for graduates (NCSC, 2018c). This follows a similar approach to the USA (Cyber Security Education, 2018). Originally initiated through master's degree certifications, it is part of the effort to raise the bar for cybersecurity skills in the UK. Universities are able to apply for assessment against the scheme through their demonstration of cybersecurity content quality, quantity of doctorates being undertaken, and critical mass of academic staff engaged in leading-edge cybersecurity research (NCSC, 2018d). These universities form the Academic Centers of Excellence (ACE) (Parr, 2014; SC Magazine, 2014). Following on from this successful implementation, NCSC are now certifying undergraduate degrees. Academic Centers for Doctoral Training have now been formed in the UK – themselves drawn from the ACE endorsed universities (NCSC, 2018e). The list of ACE universities is maintained by NCSC and updated when new universities are appended to the list (NCSC, 2018f).

## 2.6. Competitions

A number of initiatives over the past few years have used gaming to increase student engagement. They have been used to spark the interest of adolescents and entice them into thinking about a career in cybersecurity. The most well-known event is the Cyber Security Challenge, which in itself has drawn in supportive competitions such as Cyber Centurion from the USA (Cyber Security Challenge, 2018a) and Capture the Flag activities (Cyber Security Challenge, 2018b). In a similar vein the SANS Institute also runs its Cyber Discovery events in the UK (Digginns, 2018). These events and competitions follow a similar format to simulate or emulate cyber-attacks under controlled conditions. The participants are usually broken down into two teams: Red (attacker) and Blue (defender). The Cyber Security Challenge has a further tie in with the current UK Government strategy by promoting CyberFirst (Cyber Security Challenge, 2018c).

## 3. ARGUMENT FOR BLENDED LEARNING AND DEVELOPMENT

### 3.1. Discussion

Cybersecurity threats are growing in scale and effectiveness (Bird, 2015), but user awareness is a key defense (Embers, 2018). A recent massive phishing campaign has revealed the scale of the problem by targeting the USA, UK and Europe (Abel, 2018; Paganini, 2018). Reportedly, IT workers, especially millennials, are most susceptible to falling for impersonation fraud disseminated by email (Dunn, 2018). Not surprisingly this is related to the bombardment of emails with malicious intent – one in a hundred emails are a hacking attempt (Palmer, 2018). However, research estimates that 88% of UK data breaches are caused by human error, rather than by cyber-attacks (Ismail, 2018).

In effect a user's judgement whether to click that malicious link can be impaired by their busy day, absent mindedness or laziness – this problem effects both sides of the Atlantic (Tucker, 2018). In response the NCSC has decided to use technical measures to counter email spoofing in the public sector through the introduction of Domain-based Message Authentication, Reporting and Conformance (NCSC, 2017b; NCSC, 2018g). In addition, it has been identified that the education sector needs to continually invest in order to protect its networks (Kennett, 2017). For the public and private sector, technical measures need to be supplemented by explicit and implicit knowledge to facilitate effective learning (Stephanou & Daganda, 2008). However, people's attitudes and their receptiveness

to awareness training is also a factor and education should be used to influence the conditioning of human behavior (Higbee, 2017). Not only that people need to believe in the application of information security (Olusegun & Ithnin, 2013). Furthermore, effective training and learning campaigns need to be meaningful to change people's behaviors (Alexander et al., 2013).

Collaboration between academia and industry has been recommended through research conducted by the University of Westminster and includes considerations from social science (Trim et al., 2014). Although there is commonality of underpinning technical aspects, there is a perspective and paradigm shift needed to provide adequate cybersecurity training and education (Stilgherrian, 2018). The scale of the need for cybersecurity understanding extends to the use of the cloud which could be utilized by public and private sectors and the general public alike (Adams, 2017). Effectively, people require a mind-set change to avoid cybersecurity efforts being undermined. The Australian Computer Society (2016) recognized the fact that the employment of cybersecurity professionals and the training of key IT staff and managers should form part of an organization's cybersecurity readiness.

Traditionally, the cybersecurity industry demanded a badge – a qualification or certification as short-hand proof of competence and at lot of emphasis was placed on the right certification (Balaji, 2018). Some practitioners entered the IA world by carrying out self-learning and self-funded examinations to become established on the career ladder. Ten years or so ago this was an acceptable approach, where the community tended to operate under a self-help mind-set (ZDNet, 2007). With learning and development companies all vying for market position, it might be tempting for previous information security courseware to be rebadged under the cybersecurity banner. That is why the NCSC have taken the approach to vet cybersecurity providers and universities in an aligned way to meet the UK Cyber Security Strategy agenda.

Most of the classic certification examinations have either been fully or partly fulfilled by the use of multiple-choice question and answer constructs. While some certifications do require a number of years' experience as a prerequisite to take certain examinations, multiple choice exams have been criticized as not necessarily demonstrating an adequate level of skills competency (Such et al., 2015) and only show a candidate's knowledge retention capability. Debatably a key proponent of multiple-choice exams in a candidate's awareness of the certification body's exam techniques by practicing sample questions. Conversely, it would appear - depending on the topic being examined - CREST provides a combination of practical examinations, short essay and multiple-choice examination question types. OSCP is also renowned as a very reputable means of qualifying within the Pentest discipline in the private sector due to the rigor of the practical examination component. However, Coventry University has proposed that a case-study based learning approach might be more beneficial (Hendrix et al., 2016) and this is especially pertinent to gaming.

While the options in the previous section provide pieces that can contribute to a whole, CT badged courses and ACE degrees do provide extrinsic assurance that training companies and academic institutions are credible in specific cybersecurity spheres. This is especially pertinent with calls for cybersecurity to be opened up to other non-traditional information security skillsets like developers for example (Jones & O'Neill, 2017); where a cultural change is required toward secure implementation considerations in software development (Bird, 2017). As a case in point, the upsurge in the use of Internet of Things (IoT) technologies was an opportunity to reevaluate cybersecurity considerations. Notwithstanding the limitations of sensor compute and power draw, IoT has questionably become an antonym to best information security practice; that is fundamental flaws are being introduced through the misconfiguration of IoT assets (Allen, 2018). Perhaps this is why the CyBOK is placing some prominence on initially tackling cryptography and software security considerations.

### **3.1.1. Identified Challenges**

The intent of the CCP was to remedy some of the deficiencies of the CLAS scheme and become the de facto certification for the cybersecurity industry in the UK (McKinnon, 2012); it was subsequently recognized in Europe as providing good cybersecurity practice (International Telecommunications

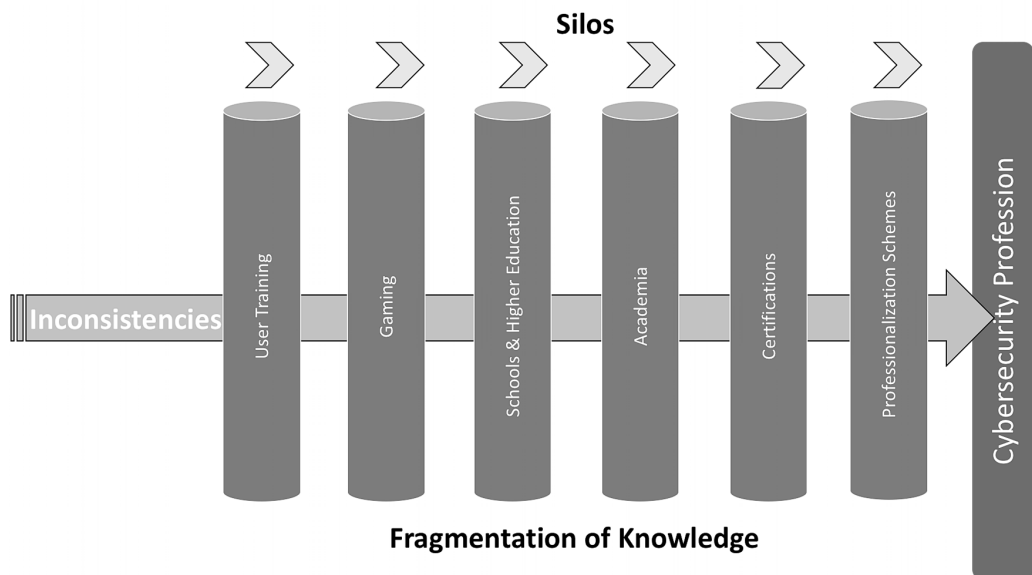


Union, 2014). However, even though CLAS was identified by academia as a mature scheme (Such et al., 2015; Bada et al., 2016) a decision was made to phase it out in a bid to purportedly strengthen the quality of consultancy for government customers and achieve a better match for government customers using the right expertise (WIREDGOV, 2015). In 2018 the NCSC reaffirmed their continued support for the CCP albeit there is recognition that specialisms should be introduced over the existing roles format; the NCSC has provided a commitment to transition the scheme for alignment with CyBOK (Anne, 2018b).

However, there exists a conundrum between qualifications and competencies; this has already been tested through various schemes such as CLAS and CCP. Inconsistencies and fragmentation of knowledge has been levied as a criticism by Industry and this is reinforced by the DCMS public consultation (Such et al., 2015; Jones & O'Neill, 2017). CyBOK is an opportunity to provide a foundational and measurable knowledge (University of Bristol, 2018) facilitated by the valued contribution of other professional bodies and institutions. That said, the change in direction towards a core body of knowledge provides an opportunity to define a centralized framework of delivery for the cybersecurity disciplines (Jones & O'Neill, 2017). The disparity of existing cybersecurity training and education efforts has been assimilated and illustrated in Figure 1.

So, before the UK commits to introducing yet another scheme, such as the proposed Chartered status, there is potentially a need to go beyond CyBOK and build a Core Knowledge Framework (CKF) of criteria; distilled across future school curricula, training courses, degrees that is so widely ranging it influences our social-technical culture; this would be a move towards what could be considered an unequivocal underpinning knowledge-based approach. Burnap (2018) has stated that there is presently no clear pathway for cybersecurity compared to other engineering disciplines. The implementation of a CKF would be considered a truly holistic education initiative to remedy his concern. Therefore, there is a case for considering how knowledge transfer will be conducted to maximize knowledge retention and to assist in future practitioner knowledge development; enabling individuals to be fulfilled and progress in a more rounded cybersecurity career. So, the question is how this could be implemented?

Figure 1. Knowledge fragmentation, silos and inconsistencies



### 3.2. Defense Systems Approach to Training Exemplar

The Defense Systems Approach to Training (DSAT) is a methodology that provides a complete framework for the analysis, design, delivery and assurance of training provided for the UK Ministry of Defense (MOD) (MOD, 2017a). It is recognized by the Public Sector and applied by consultancies undertaking public sector contracts. Therefore, it is familiar to both public and private sectors and academics in the defense industry. DSAT is best practice for the identification of training objectives, the design and development of training courseware and its oversight across the MOD. A key consideration of DSAT is blended learning as it is defined as:

*The most appropriate mix of Methods & Media which may include both traditional means, such as face-to-face in a classroom, and the use of modern learning technologies whether centralized or distributed. (MOD, 2017a)*

Blended learning - as stipulated by DSAT - is traditionally applied as a mix of instructor-led training combined with the use of virtual learning environments (MOD, 2017b). Even with the introduction of CyBOK, it is proposed that a wider knowledge framework needs to be envisaged for a truly integrated professional framework. This could be an extended version of CyBOK or CyBOK and could be the first stage towards a coherent CKF. The UK could learn from the USA's recognition that collaborative approaches in learning and development are beneficial (Williams, 2017). Reinforcing the point that mixed methods and techniques are needed for the delivery of training and education and these should be core components of a CKF. It is proposed that the CKF should be underpinned by the principles of blended learning, which could be adopted across a wider spectrum to inform the cybersecurity community learning and development strategy. Blended learning and development as a hybrid learning-delivery model could be used to join up existing silos of disparate development and delivery techniques previously highlighted in the background section. As a mechanism of delivery, a blended approach moves towards a fully integrated knowledge in practice approach and could act as the pillars to support the cybersecurity profession.

### 3.3. Blended Learning and Development Proposal

Based around a standardized and embedded CKF, where the stakeholders are working from an agreed structure, the relevant functional training and learning needs of the cybersecurity profession will be able to be discerned. This would enable the development of relevant and appropriate training and education delivery. The CKF should be interpreted and integrated at various levels of complexity and detail depending on the knowledge level implemented; for example, there are obvious differences in the depth of knowledge applied at the school level and to that at post-graduate degree standard.

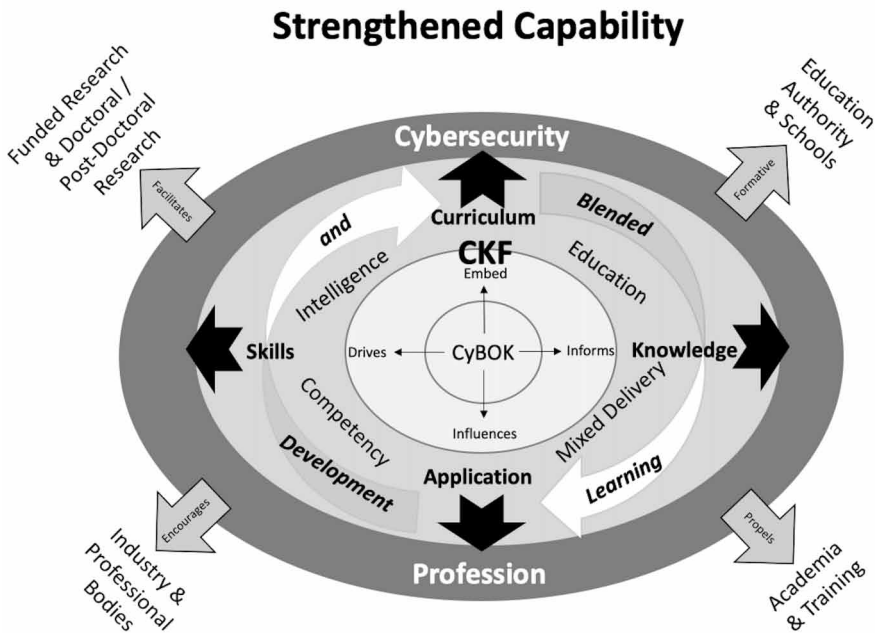
Through past lessons learned, any irregularities and subjectivity would need to be identified and removed to avoid repetitions of past inconsistencies. Therefore, it would be necessary for learning objectives to be applicable as assessment criteria and be structured in a stable format; but a CKF must also be able to evolve by taking account of any changes, enhancements and amendments of knowledge in a controlled and non-deprecating manner. Specialisms have been identified as a relevant approach for undergraduate curricula by Marymount University in the USA (Bicak, 2015). The proposed Chartered status approach also endorses such an approach. However, it is not all about the up-and-coming cybersecurity generation; in order for professionalization endeavors to be successful, the knowledge and skills of individuals already active in cybersecurity need to be drawn upon as well (Swain, 2014). There should be some emphasis regarding on-the-job training, mentoring by experienced cybersecurity practitioners and awareness from attending cybersecurity conferences.

A variety of blended learning techniques are required to avoid prohibiting different learning styles by members of the target audience and limiting choice; some prefer academia, some prefer vocational approaches, and some prefer certifications. However, the CKF needs to be embedded

and integrated across all areas of training and education; learning objectives from existing training and academic courses could be mapped against CKF criteria by the requisite training and education bodies in order to prove their correlation and relevance. The cybersecurity community should learn from the qualifying examinations implemented by CREST, OSCP and other information technology vendors who require both practical and demonstrable knowledge application. Social constructionism would be useful as it reconstructs knowledge by using an experiential method of real-world contexts, read in order to apply learning techniques to remedy specific problems (Martin-Brown, 2018); it is purported to be a step away from direct instruction techniques and could be a method that is relevant for cybersecurity knowledge transfer and reinforcement learning (Veseli, 2011).

It has been recognized by the Institution of Education at the University College London (2001) that learning can enhance performance, but conversely just focusing on performance can actually hinder performance itself. Therefore, the overall experience of professionalization for individuals must be progressive and provide obvious reward. Even though competency assessments will be required for the proposed cybersecurity Chartered status, it should not be a recycling of skillset reaffirmations already experienced through previous professionalization scheme changes. As a career pathway, initially underwritten by CyBOK it needs to remain relevant. Therefore CyBOK could in time be expanded further and developed into a CKF for the delivery of theory, practical skills application, and competencies applied in context on behalf of the profession; and would need to be constantly adaptive and expansive as shown in Figure 2. The enabler behind this CKF is blended learning and development, which can be tuned to hone the skills of practitioners and benefit the cybersecurity profession in a cyclical manner influencing the teaching of the national curriculum, training and education, academia and institutions by vocation. The cybersecurity profession, as a future career pathway, would also propagate demand in a ripple effect to inspire schools, push training companies, encourage industry involvement and generate a demand for further research efforts. Without this type of approach, the adoption and recognition of a cybersecurity profession would be limited, thereby affect its reputation and potentially digress from the main aim of establishing a proficient cybersecurity capability.

Figure 2. The influencing effects of blended learning and development



The ratios and depth and breadth of learning styles ranging from academic, vocational, practical and competitive approaches to attain the requisite knowledge under a CKF are yet to be discerned from a much-needed study. Crucially, wider information technology community engagement is required to adopt a blended training approach in order to establish the vision for a successful holistic framework.

#### 4. CONCLUSION

The more recent UK Government cybersecurity agenda is undoubtedly a step in the right direction to cultivate cybersecurity as a profession. This is very positive and provides more career opportunities under the cybersecurity banner than before. The road towards professionalization has been an audacious journey and the UK Government's agenda has been purposeful. The NCSC has played an influential role in navigating the profession towards a future state. However, there have been some issues on the path towards the UK's cybersecurity profession; a change in direction along the way has resulted in a reputable scheme being wound up and thereby spring boarded the UK cybersecurity profession onto the next step. On that basis, the evolution towards a professional pathway is erring towards CyBOK and a Cyber Security Council fulfilling a regulatory-type function. Any new Chartered status profile should also be informed by the undisputed and valuable contributions by the Cyber Security Alliance. It is important for the Cyber Security Alliance to be involved along the way and it should not be seen to be in competition with the UK Government agenda. Rather, each should complement the other in a collaborative manner to create a viable and robust framework for the cybersecurity profession.

A Cyber Security Council is perceived to be the mortar to form a firm structure to help people progress in their cybersecurity career and to provide confidence that a career in cybersecurity is fulfilling. Training and education institutions and bodies see the cybersecurity training and education market as very lucrative. Existing training courseware and education regimes, as stated in the background section, individually contribute towards this strategy; however, individually they are not the totality of knowledge comprehension but can contribute to the sum of cybersecurity understanding; this can be mapped against qualifying criteria for a holistic framework. The proposed CKF should be a wide-reaching amalgamation of knowledge objectives and thereby influence the entire training and education community. In a similar vein to the science and engineering professions, base principles need to be applied ranging across the school curriculum, through high school to graduate and post-graduate level. It must also influence certifications and competency orientated career routes such as Chartered status to ensure the future cybersecurity profession has a fully rounded knowledgeable recipe for success. Whether the CKF concept is an extension or derivation of the CyBOK or whether the CyBOK is a step towards a more coherent CKF will only be discerned from future analysis. But what is important is that there is a concerted effort between academia, industry and government to achieve a common goal of formalizing the profession.

Although there is a desire to jump onto the cybersecurity bandwagon, there needs to be buy-in by the wider target audience, a desire and mind-set change for an effective standardized structure that will be applicable to develop their career. This has already started with the NCSC stating that the following are expected to demonstrate foundation knowledge: (a) NCSC certified degree, (b) full membership of the IISP meeting their core competency criteria that underpins the CCP scheme in its current form, and (c) holding a CISSP and continued membership of (ISC)<sup>2</sup> (NCSC, 2018h); these are being mapped as a step towards rationalizing the CCP scheme for alignment with CyBOK. That said, it is recommended that we build upon this positive first step of establishing CyBOK cybersecurity specialisms and implement a wider CKF to augment the CyBOK initiative to aid knowledge and skills enhancement.

With a global deficit of three and half million cybersecurity job openings by 2021 (Stephenson, 2018), from a UK perspective a blended approach for learning and development could be used to fill the gaps and join up existing silos of training and education activities based upon a common CKF. The CKF could be a key contributory factor towards shaping the new proposed profession and facilitate

cybersecurity knowledge and skills intelligence in the UK. It is argued that this is a crucial element of learning and development and the new proposed Chartered status is only part of the puzzle. To flourish, the CKF and subsequent blended learning and development implementations must also be recognized as a credible exemplar - in order to achieve buy-in from the majority of diverse stakeholders within the cybersecurity community - and thereby sustain the cybersecurity capability within the UK.

## **ACKNOWLEDGMENT**

It is recognized that the NCSC has been crucial in steering the UK's cybersecurity training agenda. While other professional bodies and institutions have also provided leadership in the area of cybersecurity.

## REFERENCES

- Abel, R. (2018). *Massive phishing campaign targets half a billion users in the first quarter 2018*. Retrieved from [www.scmagazine.com/massive-phishing-campaign-targets-half-a-billion-users-in-the-first-quarter-2018/article/761541/](http://www.scmagazine.com/massive-phishing-campaign-targets-half-a-billion-users-in-the-first-quarter-2018/article/761541/)
- Adams, C. (2017). *IT Training Choices in a Fast-Paced World*. Retrieved from <https://www.zdnet.com/article/it-training-choices-in-a-fast-paced-world/>
- Afifi-Sabet, K. (2018). *A guide to cyber security certification and training*. Retrieved from <http://www.itpro.co.uk/careers/28212/a-guide-to-cyber-security-certification-and-training>
- Alexander, D., Finch, A., & Sutton, D. (2013). *Information Security Management Principles*. Swindon, UK: British Computer Society.
- Allen, T. (2018). *There is a massive hole in IoT security, says Avast researcher*. Retrieved from <https://www.computing.co.uk/ctg/news/3061282/there-is-a-massive-hole-in-iot-security-says-avast-researcher>
- Anne, W. (2018a). *Maturity models in cyber security: what's happening to the IAMM? NCSC*. Retrieved from <https://www.ncsc.gov.uk/blog-post/maturity-models-cyber-security-whats-happening-iamm>
- Anne, W. (2018b). *Our commitment to the CCP scheme*. Retrieved from <https://www.ncsc.gov.uk/blog-post/our-commitment-ccp-scheme>
- CREST Australia. (2017). *OSCP and CRT Equivalency*. Retrieved from [https://www.crestaaustralia.org/certification\\_crt\\_equivalency.html](https://www.crestaaustralia.org/certification_crt_equivalency.html)
- Australian Computer Society. (2016). *Cybersecurity Threats Challenges Opportunities*. Australian Computer Society.
- Bada, M., Arreguín-Toft, I., Brown, I., Cornish, P., Creese, S., Dutton, W., ... & Roberts, T. (2016). *Cybersecurity Capacity Review of the United Kingdom*. Oxford University, UK: Global Cyber Security Capacity Centre.
- Balaji, N. (2018). *A Perfect Way to Start and Strengthen Your Cyber Security Career*. *GBHackers*. Retrieved from <https://gbhackers.com/a-perfect-way-to-start-and-strengthen-your-cyber-security-career/>
- BCS. (2018). *Qualifications and certifications*. Retrieved from <https://www.bcs.org/category/5677>
- Beyer, M., Ahmed, S., Doerlemann, K., Arnell, S., Parkin, S., & Sasse, M. A. Prof., & Passingham, N. (2016). *Awareness is only the first step*. Hewlett Packard, UK: Hewlett Packard Enterprise Development LP.
- Bicak, A., Liu, M., & Murphy, D. (2015). *Cybersecurity Curriculum Development: Introducing Specialties in a Graduate Program*. *Information Systems Education Journal*, 13(3), 99–110.
- Bird, D. (2015). *Forewarned is Forearmed: Combating the Insider Threat*. UK: CyberTalk Magazine.
- Bird, D. (2017). *Prevent a menace from lurking within*. UK: CyberTalk Magazine.
- Burnap, P. (2018). *Industry Panel*. In *Proceedings of 11<sup>th</sup> International Conference on Security of Information and Networks*. Cardiff University, UK.
- Cabinet Office. (2011). *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*. London, UK: Crown Copyright.
- Cabinet Office. (2016). *National cyber security strategy 2016-2021*. London, UK: Crown Copyright.
- CESG. (2015). *The Information Assurance Maturity Model and Assessment Framework*. Cheltenham, UK: Crown Copyright.
- CESG. (2016). *CESG Certification for Cyber Security/IA Professionals*. Cheltenham, UK: Crown Copyright.
- Chris, E. (2018). *Developing the cyber security profession – have your say! NCSC*. Retrieved from <https://www.ncsc.gov.uk/blog-post/developing-cyber-security-profession-have-your-say>
- Cox, J. (2017). *UK faces dramatic cyber-security skills 'cliff edge' and is chronically under prepared for hacker attacks, study finds*. *The Independent*. Retrieved from <https://www.independent.co.uk/news/business/news/uk-cyber-security-skills-cliff-edge-under-prepared-hacker-attacks-study-multinationals-government-a7578091.html>

- CREST. (2018a). *Assurance in Information Security*. Retrieved from <https://www.crest-approved.org>
- CREST. (2018b). *CREST Registered Penetration Tester*. Retrieved from <https://www.crest-approved.org/examination/registered-tester/index.html>
- CREST. (2018c). *Collaborative Alliance of Organisations Announced to Advance the UK's Cyber Security Profession*. Retrieved from <https://www.crest-approved.org/2018/07/19/collaborative-alliance-of-organisations-announced-to-advance-the-uks-cyber-security-profession/index.html>
- Cyber Security Challenge. (2018a). *Play the Challenge*. Retrieved from <https://www.cybersecuritychallenge.org.uk>
- Cyber Security Challenge. (2018b). *Capture the Flag*. Retrieved from <https://www.cybersecuritychallenge.org.uk/competitions/capture-the-flag>
- Cyber Security Challenge. (2018c). *CyberFirst*. Retrieved from <https://www.cybersecuritychallenge.org.uk/education/further-education/cyber-first>
- Cyber Security Education. (2018). *CYBER SECURITY COURSES*. Retrieved from <https://www.cybersecurityeducation.org/courses/>
- Dallaway, E. (2017). IISP Apply to Privy Council for Information Security Royal Charter. *Info Security Magazine*. Retrieved from <https://www.infosecurity-magazine.com/news/iisp-apply-royal-charter/>
- DCMS. (2017). *5. A safe and secure cyberspace - making the UK the safest place in the world to live and work online*. Retrieved from <https://www.gov.uk/government/publications/uk-digital-strategy/5-a-safe-and-secure-cyberspace-making-the-uk-the-safest-place-in-the-world-to-live-and-work-online>
- DCMS. (2018). *Developing the UK cyber security profession*. Retrieved from <https://www.gov.uk/government/consultations/developing-the-uk-cyber-security-profession>
- DeGroat, T. J. (2018). 5 Cybersecurity Certifications That Will Help You Land a Job. *Springboard*. Retrieved from <https://www.springboard.com/blog/cybersecurity-certifications/>
- Department for Digital, Culture, Media and Sport. (2018). *Cyber Security Breaches Survey 2018*. Crown.
- Diggins, A. (2018). Final stage of Cyber Discovery finishes in London. *EdTechnology*. Retrieved from <https://edtechnology.co.uk/Article/final-stage-of-cyber-discovery-finishes-in-london>
- Diggins, A. (2018). Final stage of Cyber Discovery finishes in London. *Edtechnology*. Retrieved from <https://edtechnology.co.uk/Article/final-stage-of-cyber-discovery-finishes-in-london>
- Dunn, J. (2018). Feel the shame: Email-scammed staffers aren't telling bosses about it. *The Register*. Retrieved from [https://www.theregister.co.uk/2018/09/07/scam\\_business\\_emails\\_on\\_the\\_rise/](https://www.theregister.co.uk/2018/09/07/scam_business_emails_on_the_rise/)
- Embers, R. (2018). Security: The Rules of Engagement to Mitigate Insider Risk. *Security Boulevard*. Retrieved from <https://securityboulevard.com/2018/08/security-the-rules-of-engagement-to-mitigate-insider-risk/>
- Finch, A., & Furnell, S. (2018). Is this the year for the Security Professional. *Infosecurity Europe*. Retrieved from [http://www.infosecurityeurope.com/\\_\\_novadocuments/486575?v=636657836899000000](http://www.infosecurityeurope.com/__novadocuments/486575?v=636657836899000000)
- Finch, A., Glover, I., & Smith, R. (2018). Does the UK Need an Information Security Royal Charter? *Info Security Magazine*. Retrieved from <https://www.infosecurity-magazine.com/magazine-features/uk-information-security-royal/>
- GoCertify. (2018). *ISACA Study Addresses Global Cybersecurity Challenges*. Retrieved from <http://www.gocertify.com/articles/isaca-study-addresses-global-cybersecurity-challenges>
- Great Schools Partnership. (2014). *Blended Learning*. Retrieved from <https://www.edglossary.org/blended-learning/>
- Grout, V. (2015). *Cybersecurity to Become Core Component of UK Computing Degrees*. Retrieved from <https://cphc.ac.uk/2015/06/29/cybersecurity-to-become-core-component-of-uk-computing-degrees/>
- Hendrix, M., Al-Sherbaz, A., & Bloom, V. (2016). Game Based Cyber Security Training: Are Serious Games suitable for cyber security training? *International Journal of Serious Games*, 3(1), 52–61. doi:10.17083/ijsg.v3i1.107

Higbee, A. (2017). Cyber security education: Why we need to re-think it. *Training Journal*. Retrieved from <https://www.trainingjournal.com/articles/opinion/cyber-security-education-why-we-need-re-think-it>

IA Advisory Council. (2016). Free 'Introduction to cyber security' course launched.' Retrieved from <https://www.iaac.org.uk/free-introduction-to-cyber-security-course-launched/>

IISP. (2018). Accredited Training Courses. Retrieved from [https://www.iisp.org/imis15/iisp/Accreditation/Accredited\\_Training/iispv2/Accreditation/Accredited\\_Training.asp](https://www.iisp.org/imis15/iisp/Accreditation/Accredited_Training/iispv2/Accreditation/Accredited_Training.asp)

ISACA. (2015). State of Cybersecurity: Implications for 2016. In *ISACA and RSA Conference Survey, Elsevier Computers & Security*.

ISACA. (2017). *Survey: Cyber Security Skills Gap Leaves 1 in 4 Organizations Exposed for Six Months or Longer*. Retrieved from [http://www.isaca.org/About-ISACA/Press-room/News-Releases/2017/Pages/Survey-Cyber-Security-Skills-Gap-Leaves-1-in-4-Organizations-Exposed-for-Six-Months-or-Longer.aspx?utm\\_referrer=](http://www.isaca.org/About-ISACA/Press-room/News-Releases/2017/Pages/Survey-Cyber-Security-Skills-Gap-Leaves-1-in-4-Organizations-Exposed-for-Six-Months-or-Longer.aspx?utm_referrer=)

ISACA. (2018). State of Cybersecurity 2018 Part 1: Workforce Development.

Ismail, N. (2018). Cyber security training: Is it lacking in the enterprise? Retrieved from <https://www.information-age.com/cyber-security-training-123474550/>

ITU. (2014). Global Cybersecurity Index – Good Practices. International Telecommunications Union.

Jones, N., & O'Neill, L. (2017). *The Profession*. Swindon, UK: Information Assurance Advisory Council.

Kennett, S. (2017). Cyber security: why the education sector can't afford not to invest. Retrieved from <https://www.jisc.ac.uk/blog/cybersecurity-why-the-education-sector-cant-afford-not-to-invest-13-apr-2017>

Kleinman, L. (2018). Cybersecurity And The New CISO: The Leadership Enigma. *Forbes*. Retrieved from <https://www.forbes.com/sites/forbestechcouncil/2018/07/26/cybersecurity-and-the-new-ciso-the-leadership-enigma/#2abe5fc43422>

Knowles, W., Baron, A., & McGarr, T. (2016). The Simulated Security Assessment Ecosystem: Does Penetration Testing Need Standardisation? *Computers & Security*, 1–22.

MacWillson, A. (2018). UK cyber economy will rise to £2bn by 2016, aided by partnerships with Facebook and BT. *Realwire*. Retrieved from <https://www.realwire.com/releases/IISP-Launches-New-Skills-Framework-for-Information-Security-Professionals>

Magazine, S. C. (2014). GCHQ certifies six MSc cyber security degrees. *SC Magazine*. Retrieved from <https://www.scmagazineuk.com/gchq-certifies-six-msc-cyber-security-degrees/article/1480937>

Martin-Brown, G. (2018). *Personalised learning & the future of education [YouTube video]*. Retrieved from [https://www.youtube.com/watch?v=j\\_eb4TwdW0o](https://www.youtube.com/watch?v=j_eb4TwdW0o)

Mashable, U. K. (2018). Switch to a career in cybersecurity by taking these online classes. *Mashable*. Retrieved from <https://mashable.com/2018/04/17/cyber-security-certifications-online-classes/?europa=true>

McDonald, C. (2018). Average technology salary in UK&I reaches over £80,000. *Computer Weekly*. Retrieved from <https://www.computerweekly.com/news/252448472/Average-technology-salary-in-UKI-reaches-over-80000>

McKinnon, I. D. (2012). *Information Security Group. Review 11/12. Royal Holloway*. UK: University of London.

Milligan, R., & Rajab, T. (2015). CESG launch new Certified Cyber Security Consultancy scheme. *TechUK*. Retrieved from <http://www.techuk.org/insights/news/item/4529-cesg-launch-new-certified-cyber-security-consultancy-scheme>

MOD. (2017a). *JSP 822 Defence Direction and Guidance for Training and Education Part 2. Ministry of Defence*. UK: Crown Copyright.

MOD. (2017b). *JSP 822 Defence Direction and Guidance for Training and Education Part 1. Ministry of Defence*. UK: Crown Copyright.

Morgan, S. (2017). Please don't send me to cybersecurity training. *CSOOnline*. Retrieved from <https://www.csoonline.com/article/3225471/security/please-dont-send-me-to-cybersecurity-training.html>



- Murphy, I. (2017). NCSC appeals for students to takes its money. *Enterprise Times*. Retrieved from <https://www.enterprisetimes.co.uk/2017/11/17/ncsc-appeals-students-takes-money/>
- NCSC. (2016). Cyber Security Consultancy. Retrieved from <https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy>
- NCSC. (2017a). CHECK Fundamental Principles. Retrieved from <https://www.ncsc.gov.uk/articles/check-fundamental-principles>
- NCSC. (2017b). Email security and anti-spoofing. Retrieved from <https://www.ncsc.gov.uk/guidance/email-security-and-anti-spoofing>
- NCSC. (2018a). GCHQ Certified Training. Retrieved from <https://www.ncsc.gov.uk/scheme/gchq-certified-training>
- NCSC. (2018b). *Cyber Security Consultancy Standard*. London, UK: Crown Copyright.
- NCSC. (2018c). Certified cyber security courses. Retrieved from <https://www.prospects.ac.uk/jobs-and-work-experience/job-sectors/law-enforcement-and-security/certified-cyber-security-courses>
- NCSC. (2018d). Academic Centres of Excellence in Cyber Security Research. Retrieved from <https://www.ncsc.gov.uk/articles/academic-centres-excellence-cyber-security-research>
- NCSC. (2018e). NCSC-certified degrees. Retrieved from <https://www.ncsc.gov.uk/information/ncsc-certified-degrees>
- NCSC. (2018f). Certified Training Courses. Retrieved from <https://www.ncsc.gov.uk/information/certified-training-courses>
- NCSC. (2018g). NCSC Mail Check. Retrieved from <https://www.ncsc.gov.uk/mailcheck>
- NCSC. (2018h). Setting new foundations for the CCP scheme. Retrieved from <https://www.ncsc.gov.uk/blog-post/setting-new-foundations-ccp-scheme>
- Nepal, S. (2018). Building Trustworthy IoT-Cloud Data Lifecycle. In *Proceedings of 11<sup>th</sup> International Conference on Security of Information and Networks*, Cardiff University, UK.
- Nicholls, D. (2018). *Veterans to be retrained as cyber warriors, under new partnership backed by the MoD*. Retrieved from <https://www.telegraph.co.uk/news/2018/08/11/veterans-retrained-cyber-warriors-new-partnership-backed-mod/>
- Oesch, T. (2018). Diversifying the Cybersecurity Workforce With Learning and Development. *Training Industry*. Retrieved from <https://trainingindustry.com/articles/it-and-technical-training/diversifying-the-cybersecurity-workforce-with-learning-and-development/>
- Office of National Statistics. (2011). 2011 Census Security: Report of the Independent Review Team. Retrieved from <https://www.ons.gov.uk/census/2011census/confidentiality/assessingourmeasurestoprotectyourconfidentiality>
- Olusegun, O. J., & Ithnin, N. B. (2013). People Are the Answer to Security: Establishing a Sustainable Information Security Awareness Training (ISAT) Program in Organization. *International Journal of Computer Science and Information Security*, 11(8).
- Open University. (2018). Introduction to Cyber Security. Retrieved from <https://www.futurelearn.com/courses/introduction-to-cyber-security>
- Osborne, G. (2015). Chancellor's speech to GCHQ on cyber security. Retrieved from <https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security>
- Paganini, P. (2018). Iran-linked COBALT DICKENS group targets universities in new phishing campaign. *Security Affairs*. Retrieved from <https://securityaffairs.co/wordpress/75710/cyber-warfare-2/cobalt-dickens-iran-attacks.html>
- Palmer, D. (2016). Training? What training? Workers' lack of cybersecurity awareness is putting the business at risk. *ZDNet*. Retrieved from <https://www.zdnet.com/article/training-what-training-workers-lack-of-cybersecurity-awareness-is-putting-the-business-at-risk/>

Palmer, D. (2018). Phishing warning: One in every one hundred emails is now a hacking attempt. *ZDNet*. Retrieved from <https://www.zdnet.com/article/phishing-warning-one-in-every-one-hundred-emails-is-now-a-hacking-attempt/>

Parr, C. (2014). First GCHQ-certified master's courses unveiled. *Times Higher Education*. Retrieved from <https://www.timeshighereducation.com/news/first-gchq-certified-masters-courses-unveiled/2014921.article>

Pop, A. (2018). What's the Difference Between Blended Learning, E-Learning and Online Learning? *Distance Learning*. Retrieved from <https://www.distancelearningportal.com/articles/269/whats-the-difference-between-blended-learning-e-learning-and-online-learning.html>

Rashid, A., Danezis, G., Chivers, H., Lupu, E., & Martin, A. (2018). Scope for the Cyber Security Body of Knowledge. University of Bristol, UK: CyBOK.

Ryan, G. (2018). *Stem vital to UK's future cybersecurity*. Retrieved from <https://www.tes.com/news/stem-vital-uks-future-cybersecurity>

SANS. (2018). *World Leading Cyber Security Training*. Retrieved from <https://uk.sans.org>

Schneier, B. (2013). *Is Cybersecurity a Profession?* Retrieved from [https://www.schneier.com/blog/archives/2013/10/is\\_cybersecurit.html](https://www.schneier.com/blog/archives/2013/10/is_cybersecurit.html)

Stephanou, T., & Dagada, R. (2008). The Impact of Information Security Awareness Training on Information Security Behaviour: The Case for Further Research. In *Proceedings of ISSA 2008 Innovative Minds Conference*.

Stephenson, M. (n.d.). Insecurity Podcast: Joe Billingsley on Cyber Education and the Modern Military. *Threat Vector*. Retrieved from [https://threatvector.cylance.com/en\\_us/home/insecurity-podcast-joe-billingsley-on-cyber-education-and-the-modern-military.html](https://threatvector.cylance.com/en_us/home/insecurity-podcast-joe-billingsley-on-cyber-education-and-the-modern-military.html)

Stevenson, A. (2013). UK cyber economy will rise to £2bn by 2016, aided by partnerships with Facebook and BT. *V3*. Retrieved from <https://www.v3.co.uk/v3-uk/news/2318616/uk-cyber-economy-will-rise-to-gbp2bn-by-2016-aided-by-partnerships-with-facebook-and-bt>

Stilgherrian. (2018). Security training is useless unless it changes behaviours. *ZDNet*. Retrieved from <https://www.zdnet.com/article/security-training-is-useless-unless-it-changes-behaviours/>

Such, J. M., Gouglidis, A., Knowles, W., Misra, G., & Rashid, A. (2015). *The Economics of Assurance Activities* (Technical Report SCC-2015-03). Security Lancaster, Lancaster University.

Swain, N. D. (2014). A Multi-Tier Approach to Cyber Security Education, Training, and Awareness in the Undergraduate Curriculum (CSETA). In *Proceedings of 121st ASEE Annual Conference & Exposition*, Indianapolis, IN.

The Engineer. (2016). *New cyber security qualification for the UK*. Retrieved from <https://www.theengineer.co.uk/new-cyber-security-qualification-for-the-uk/>

TheBigChoice.com. (2018). *CyberFirst Apprenticeships*. Retrieved from <https://www.thebigchoice.com/Apprenticeships/CyberFirst>

Thomas, K. (2018). Women in tech: the IT firms tackling the gender imbalance. *The Guardian*. Retrieved from <https://www.theguardian.com/education/2018/jul/09/women-tech-it-technology-firms-tackling-gender-imbalance>

Tigerscheme. (2018). *Tigerscheme Qualifications*. Retrieved from <https://www.tigerscheme.org/qualifications.php>

Tittel, E., & Lindros, K. (2018). *Best Information Security Certifications 2018*. Retrieved from <https://www.businessnewsdaily.com/10708-information-security-certifications.html>

Trim, P. R., Lee, Y., Ko, E., & Kim, K. H. (2014). *Cyber security culture and ways to improve security management*. UK: University of Westminster.

Tucker, E. (2018). Cyber security – why you're doing it all wrong. *Computer Weekly*. Retrieved from <https://www.computerweekly.com/opinion/Cyber-security-why-youre-doing-it-all-wrong>

University College London. (2001). *Learning about Learning enhances performance*. UK: Institute of Education, University College London.

University of Bristol. (2018). *The Cyber Security Body Of Knowledge*. Retrieved from [www.cybok.org](http://www.cybok.org)

US Department of Education. (2018). *Science, Technology, Engineering and Math: Education for Global Leadership*. Retrieved from <https://www.ed.gov/stem>

Veseli, I. (2011). *Measuring the Effectiveness of Information Security Awareness Program*. Gjøvik, Norway: Department of Computer Science and Media Technology.

Viveros, M. (2013). Cyber Security Depends on Education. *HBR*. Retrieved from <https://hbr.org/2013/06/cyber-security-depends-on-educ>

Wikipedia. (2018). Offensive Security Certified Professional. Retrieved from [https://en.wikipedia.org/wiki/Offensive\\_Security\\_Certified\\_Professional](https://en.wikipedia.org/wiki/Offensive_Security_Certified_Professional)

Williams, C. (2017). *Building a Capable Cybersecurity Workforce through Collaborations*. National Institute for Standards and Technology. US: National Initiative for Cybersecurity Education.

Williams, H. (2017). UK government to deliver 'cyber curriculum' to tackle cyber security skills gap. *CBR Online*. Retrieved from <https://www.cbronline.com/cybersecurity/uk-government-cyber-curriculum-tackle-cyber-security-skills-gap/>

WIREDGOV. (2015). *Certification of IA industry consultancy is changing*. Retrieved from <https://www.wiredgov.net/wg/news.nsf/articles/Certification+of+IA+industry+consultancy+is+changing+03032015152000?open>

ZDNet. (2007). *Take responsibility for your own training*. Retrieved from <https://www.zdnet.com/article/take-responsibility-for-your-own-training/>

*David Bird has worked in multiple technical disciplines within both the public and private sectors for over 33 years. Over the past 11 years David has worked on many complex consortia-based projects and programs for a number of leading IT integration companies as an information security specialist. He also brings to bear his additional experience in business and training consultancy as well as performing cybersecurity research in his own time. He has had many articles published in several reputable magazines comprising topical, technical and information security subject matter that includes: British Computer Society ITNoW and Digital Leaders editions, CyberTalk and the Institute of Information Security Professionals Pulse Magazine. David has also provided a published chapter entitled 'The collaborative effects of cyberspace' in a book published by the Institute of Scientific and Technical Communicators. In 2018, he published two papers in the IEEE Xplore and ACM digital libraries.*

*John Curry is a senior lecturer in games development and cyber security at Bath Spa University. He has an international reputation in conflict simulations/ serious games and has worked with many of the key personalities in the field. He has been leading umpire in numerous cyber wargames from individual companies to state level. He co-authored handbooks on the development of new methods of serious gaming including Matrix Games and Confrontation Analysis. His professional life consists largely of using games to explore complex situations looking for insights.*