Cyber Security Education, Qualifications and Training

Prof. Keith M. Martin Information Security Group, Royal Holloway, University of London, Egham, Surrey TW20 0EX, UK

Official version, 1st published in June 2015, doi: 10.1049/etr.2014.0029, ISSN 2056-4007, www.ietdl.org

Abstract

The rise in significance of cyber security has led to an increase in the range of interesting career paths that can be followed in this area. Inevitably there has also been an explosion in the diversity of available cyber security education, qualifications and training, most of which is targeted at those seeking to engage with this promising job market. In this article, some guidelines are provided on how to select appropriate education, qualifications and training in cyber security, alongside a review of some of the many current offerings and how to differentiate between them. While the focus is on the UK cyber security sector, many of the observations have wider relevance.

Introduction

The cyber security profession is growing and there are an increasing number of fascinating ways of making a career in cyber security. As organisations have embraced the many benefits of moving their infrastructures and businesses online, there has been growing awareness of the need to manage the cyber security risks that arise. Recent years have seen both an increase in the need for general organisations employ their own cyber security specialists, as well as an expansion of the cyber security service provision sector [1].

A 2014 UK Government report [2] presented the findings of an exercise to determine the needs of business with respect to cyber security skills. It highlighted ‘a demand amongst businesses for more professionals with a range of technical skills, but also a demand for new entrants with stronger business skills and greater work experience’. It also identified ‘the importance of increasing cyber skills among those who create, purchase and use technology to reduce business vulnerability to cyber attack, and among company decision makers who are responsible for managing business risks’.

Although it has been possible to follow a career in cyber security outside of government for several decades, the current rapid expansion of the industry has taken place ahead of any mature notion of professionalization in the industry. The ‘UK Cyber Security Strategy’ [3] has helped to consolidate and galvanise attempts to develop a stronger notion of what it means to be a cyber-security professional and to identify different cyber security roles.

A career in cyber security naturally requires relevant skills and competence. In the absence of a fully mature framework for identifying these, an abundance of different education and training (generically referred to here as ‘upskilling’) offerings are available, some of which lead to formal

qualifications. One of the challenges for anyone seeking to prepare themselves for entering, or developing, a cyber-security career is which of those to pursue.

Note that throughout this article no attempt is made to distinguish between the terms ‘cyber security’ (a relatively recent nomenclature) and the more established terms ‘information security’ and ‘information assurance’. While arguments can be made about subtle differences between these, for the purposes of this article they are regarded as the same.

After a short discussion on identifying needs, this article will, in turn, examine cyber security education, qualifications and training from academia, professional bodies and the commercial sector.

Identifying Needs

The first step towards identifying how to upskill in cyber security is to identify needs. In terms of cybersecurity careers, here are some issues worth considering in advance of researching education or training in this area:

- *Type of qualification*. A fundamental decision to make is whether a formal qualification is sought. Upskilling programmes offer a range of qualifications, including academic degrees and professional certifications. On the other hand, it may be that knowledge acquisition suffices.

- *Resource commitment*. It is worth identifying the resources required to complete an upskilling programme. The financial cost is of course one resource, but perhaps more significant is the time.

- *Delivery mode*. The mode of delivery is likely to be an important factor. Some programmes require a block of time away from work, others require a longer commitment of less time (day release), while others can be conducted remotely (distance or online learning).

- *Prerequisite knowledge*. A good upskilling programme should make it clear what prerequisite knowledge is required. Some programmes assume some existing cyber security expertise, while others may be entry level.

- *Breadth of knowledge sought*. There are relatively few upskilling programmes that provide an overall foundation. Most provide a level of specialisation or have a particular focus. It is important to identify what is required and how closely an offering matches this.

- *Role-based or subject-based*. It is worth considering whether a particular cyber security career role is being sought, such as Chief Information Security Officer, or whether focused subject expertise is wanted, such as for penetration testing. Many upskilling programmes are targeted at specific roles and/or subjects.

- *Knowing or doing*. It may be important to identify the extent to which upskilling needs relate to acquiring the ‘knowledge of how to do something’, as opposed to acquiring an ability to ‘demonstrate that a particular skill has been applied in practice to a certain competency level’. Many upskilling programmes offer a combination of both, but some focus on ‘knowing’ while others focus on ‘doing’ (it is quite possible and acceptable to provide one of these during upskilling and not the other).

- *Government or private sector*. There are some differences between the requirements for certain government and private sector career options. It is worth considering whether either of these employment sectors is being explicitly considered.

- *Technology specificity*. Some upskilling programmes relate directly to specific technologies or are at least biased towards them.

Institute of Information Security Professionals (IISP) Skills Framework

Although it was noted that there was no mature framework for identifying relevant skills for a career in cyber security, in 2010 the IISP [4] established the IISP Information Security Skills Framework [5]. This identifies 'a range of competencies expected of Information Security and Information Assurance Professionals in the effective performance of their roles' and was developed through collaboration between established professionals in the public and private sectors, as well as academia. In many senses this is the best cyber security benchmarking framework that exists (certainly in the UK).

The IISP Skills Framework is based around the following competency areas, noting that not all roles require expertise in all categories:

- Information security management,
- Information risk management,
- Implementing secure systems,
- Information Assurance Methodologies and Testing,
- Operational Security Management,
- Incident Management,
- Audit, Assurance and Review,
- Business Continuity Management,
- Information Systems Research.

The IISP Skills Framework has proved influential, particularly in areas of government. The UK has a 'National Cyber Security Programme', which is intended to implement the UK Cyber Security Strategy. This includes a mission to develop knowledge, capability and skills in cyber security, much of which is developed through CESG, the UK National Technical Authority for cyber security and the more public-facing part of GCHQ. As part of this initiative the 'CESG Certified Training (CCT) Scheme' [6] is attempting to assure high quality cyber security upskilling programmes by certifying specific programmes against the IISP Skills Framework. Likewise, a variation of the IISP Skills Framework is being used to benchmark 'GCHQ Certified Master's degree programmes in cyber security' [7].

Education against Training

Much has been written about the general differences between 'education' and 'training' and most remarks about this apply as well to cyber security as to other disciplines (e.g. see [8]).

Crudely speaking, education is more focused on the acquisition of knowledge and understanding, through which skills are developed. On the other hand, training tends to be targeted at the acquisition of skills to a demonstrable level of competence. There is a strong case for engaging in both education and training as part of career development in cyber security. Perhaps this is best illustrated by example. Consider the case of someone tasked with taking on a new role overseeing the management of cryptographic keys for an organisation.

A decent education programme in the area of key management should equip the employee with a sound understanding of the principles behind cryptography, its functionality and limitations, the significance of key management, an understanding of key lifecycles, an overview of hardware security modules (HSMs) and so on. This education should give the employee a very clear understanding of the role that key management plays within the wider cyber security strategy of any organisation. What an education programme is unlikely to provide is hands-on experience of, for example, managing keys using the specific HSM technology deployed by the organisation. Indeed, it is probably unlikely to have given the employee hand-on experience of using any HSM technology.

This is the gap often filled with training programmes. These are more likely to offer hands-on experience and, in many cases, deal with very specific technologies. On a suitable training programme, the employee will hopefully learn how to operate and command a specific type of HSM. They might also learn how to develop policies and procedures for governing keys within the organisation and so on.

It should be clear that, depending on existing knowledge, both education and training are relevant. A new employee might require both. A new graduate with an education in cryptography might require training. An experienced key manager from another organisation might require training on the specific systems in use. And an existing employee with some hand-on experience might well require education in order to better understand the role and prepare to take on more responsibilities.

Crucially, a significant role of education, through delivery of the fundamentals, is to prepare someone for the future. Once you understand the fundamentals of key management you are well equipped to tackle future. developments. Training is much more about the here and now. In cyber security, as in other fields, education and training complement one another very comfortably. Progression in the cyber security profession can be aided by prudent engagement in both activities.

Academic Qualifications

A large number of upskilling programmes in cyber security are provided by academic institutions. This has particularly been so since the establishment of the UK National Cyber Security Programme, which has incentivised academic institutions to engage in cyber security activities.

Why study an academic cyber security programme?

There are probably three main reasons for considering an academic upskilling programme:

1. *Qualifications*. Academic institutions provide recognised qualifications. The quality of that qualification depends on the reputation of the specific programme and the institution behind it.

2. *Educational focus*. Academic institutions have a central mission to provide education and tend to be experienced as equipping people with fundamental skills uncluttered by the details of a particular organisational setting.

3. *Neutrality*. Academic institutions are often regarded as providing a neutral perspective free from commercial vested interests.

Certification of Institutions and Programmes

Owing to the relative explosion in the number of cyber security degree programmes, the UK Government is currently engaging in a set of certification activities designed to identify academic institutions and programmes that meet a number of quality benchmarks.
These are:

- *Academic Centres of Excellence in Cyber Security Research* [9]. This status has been awarded to institutions which are engaged in world class research in cyber security. Acquisition of Academic Centre of Excellence in Cyber Security Research (ACE-CSR) status requires not just quality in research, but also established pedigree over a span of time and critical mass of research activity. Maintenance of this status is subject to periodic review. As of 2015 there are 13 ACE-CSR institutions, with further assessments anticipated in the future.

- *Certified Master's degrees in Cyber Security* [7]. This status is awarded to Master's degree programmes that meet quality thresholds in terms of coverage and teaching. The first set of certified Master's degrees was for programmes that provide a general education in cyber security. There are currently only four programmes that have full certified status and two withprovisional certified status. There are plans to certify more focused Master's programmes, with the first such initiative being for programmes specialising in the area of digital forensics.

- *Academic Centres of Excellence in Cyber Security Education*. An invitation to academic institutions to apply for this status is anticipated in 2015, with the holding of at least one Certified Master's degreeexpected to be a prerequisite.

Choosing an academic programme

There are many different academic cyber security upskilling programmes on the market. The following criteria may be worth considering when assessing suitability of a specific offering. For another perspective on selecting academic programmes in cyber security see [10].

Type of programme. Fundamentally, the type of programme sought needs to be determined. The main classes of the degree programme are discussed shortly.

- *Cyber security focus*. It is worth carefully checking the syllabus of degree programmes with 'security' in their titles, since many academic institutions offer flavours of more general degrees that may qualify for a 'security' label with only a small security component.

- *Reputation of the programme*. Probably the most important criteria are the reputation of the programme. Certification (if applicable) is certainly an indicator of this reputation, but is also worth determining by conducting some basic research. What have past graduates said about it in public fora? Are employers familiar with it? How many graduates does it have? What are they doing now?

- *Capability of the teaching team*. The quality of teaching is an important factor and care should be taken to establish the capability of the team that will deliver the programme. A healthy diversity of teaching staff with cyber security interests is a good measure of this.

- *External connections*. The depth and breadth of external (industrial, government and other) connections are a good measure of programme reputational quality. Cyber security is a practical discipline and a good programme should be embedded in the wider cyber security community.

- *Research activity*. Engagement in quality cyber security research suggests a strong environment within which to receive cyber security upskilling. Evidence of quality publications and projects is the best indicator of this, with institutional ACE-CSR certification providing an indication of critical mass.

- *Delivery mode*. All academic programmes require substantial time commitments and many require fulltime study. Some, however, are 'friendlier' towards student's already in employment and may offer a range of part-time delivery options, such as block teaching and distance learning.

Research degrees

Research degrees require the most specialised ability and greatest time commitment. They have high entry requirements and are targeted at anyone considering a career where research skills are required. The standard research degree is the 3-year PhD programme. All ACE-CSR institutions are required to have an established and active PhD programme in place. The UK National Cyber Security Programme has funded two Centres for Doctoral Training (CDTs) in Cyber Security (at University of Oxford [11] and Royal Holloway, University of London [12]). These CDTs provide an additional first year of cohort-based structured taught cyber security training in advance of the 3-year research component.

Master's degrees

By far the most popular type of dedicated degree programme in cyber security is a Master's, which is typically 1-year fulltime or 2-year part-time. Many of these programmes are well-established and have a strong track record of preparing students for cyber security careers [13].

Relatively few Master's degree programmes provide a general balanced coverage of cyber security backed up by a strong delivery environment. The Certified Master's degree in Cyber Security initiative [7] has thus far identified just four fully-certified programmes (at Edinburgh Napier University, Lancaster University, University of Oxford, and Royal Holloway, University of London).

A number of Master's programmes focus on specialised aspects of cyber security. These may be appropriate for a student with a clear specialisation in mind, however, no certification process has yet been completed for any of these types of programme. Examples of specialist programmes include Digital Forensics (Cranfield University), Cybercrime (University of Derby) and Security Management (City University), but there are many more.

It is worth noting that a small number of Master's programmes can be conducted by distance learning and hence fitted around work commitments. Examples include Edinburgh Napier and Royal Holloway, University of London.

Undergraduate degrees

There are a number of 3-year undergraduate degree programmes in topics relating to cyber security. It is at least contestable whether degrees at this level dedicated to cyber security make complete sense, since cyber security is perhaps best understood within a wider context. Perhaps the most critical features of such programmes to consider are whether they offer balanced coverage of cyber security and whether they provide the broad range of transferable skills expected from a more traditional undergraduate degree programme. An example of a programme that appears to offer these strengths is the BSc Computer and Information Security at Plymouth University.

Perhaps undergraduate programmes are more prevalent in more traditional disciplines that offer a component of cyber security specialisation. While all modern programmes in areas such as computer science should include coverage of some cyber security, some programmes offer more substantive coverage. In the absence of any formal certification of such programmes, broader institutional activity in cyber security is a useful indicator of quality of cyber security coverage.

Diplomas and certificates

Some academic institutions offer certificates or diplomas in cyber security related topics. These are seen as a much lighter qualifications than degree programmes. These qualifications are also much more ambiguous in terms of what they represent (these terms are sometimes used for exit qualifications for partially completed higher degrees), as well as being easily confused with non-academic programmes.

Open online courses

A number of platforms offer free university courses in cyber security. These are typically short taster courses that can be studied free over the Internet. In some cases a certificate of completion can be obtained. Examples include:

- *Coursera* [14]. This is arguably the leading open learning platform and offers a small range of free cyber security courses from partner institutions around the world, including Stanford, University of Maryland University of London.

- *FutureLearn* [15]. This platform is owned by the Open University and offers programmes from a large range of academic institutions in the UK. In particular, it hosts an 'Introduction to Cyber Security', which was developed by the Open University as part of the UK national Cyber Security Programme. This course is CCT certified.

- *iTunes U*. A range of educational audio and video podcasts on cyber security topics, including lectures and interviews, are available from institutional sites hosted by iTunes U.

Professional Qualifications

Another major source of cyber security upskilling programmes relate to qualifications provided by professional bodies. Professional qualifications tend to assess both the knowledge and the ability to put knowledge into practice, with many qualifications targeted at very specific professional roles. There are fewer of these qualifications than academic programmes, so choosing between them is more straightforward. Since these are in many ways complementary to, academic programmes it is common for cyber security professionals to hold several professional qualifications as well as an academic degree. Some of the main professional bodies issuing qualifications in cyber security are as follows.

BCS

The 'BCS' [16] has been in existence for over 50 years and is the chartered institute for IT. There are a number of Special Interest Groups for aspiring cyber security professionals. The BCS provides development opportunities at a broad range of career levels through events and qualifications. Full membership confers professional status and can be reinforced through the Chartered IT Professional status. The BCS offers a small number of certifications at both foundation and practitioner levels. The BCS is also one of the three certification bodies for the CESG Certified Professional (CCP) scheme.

CESG

The CCP scheme [17] is the UK Government's approved standard for assessing cyber security professionals. The CCP scheme covers seven formally defined roles in cyber security and assesses them to four different skill levels. These roles are security and information risk advisor, information assurance architect, accreditor, information assurance auditor, IT security officer, communications and security officer, and penetration tester. Applicants for CCP certification can be independently assessed by one of three separate approved certification bodies (APM Group, BCS and IISP/CREST/Royal Holloway).

CESG also operates the 'CESG Listed Advisor' scheme [18] which identifies and support consultants who provide information security advice to central government. Membership is highly regarded in the government sector.

CREST

'CREST' [19] is an example of a professional body focused around one type of career within cyber security, namely ethical hacking and allied capabilities in the commercial sector. CREST offers a full suite of very specific qualifications that assess competency in specific roles, such as 'CREST Registered Penetration Tester', 'CREST Certified Web Application Tester' and 'CREST Registered Intrusion Analyst'.

IISP

The IISP [4] was established in 2006 to provide a professional body focused on supporting cyber security professionals. While it does not itself directly provide qualifications, it is highly influential in the cyber security upskilling space as it established the IISP Skills Framework [3] and supports CCP certification. The IISP provides a variety of membership levels, which are awarded on the basis of knowledge, experience and competence.

ISACA

'ISACA' [20] is a US-based international membership and certification organisation which has been in operation for over 40 years. It is globally successful with over 200 chapters throughout the world. The focus of ISACA is audit and control of Information Systems. ISACA provides a range of services to aspiring professionals, including several relevant certification programmes in the area of cyber security:

- *Certified Information Systems Auditor* (CISA). The CISA certification is globally recognised and is probably the most important benchmarking certificate for cyber security professionals involved in auditing and monitoring information systems.

- *Certified Information Security Manager* (CISM). The CISM certification is focused on security management and widely recognised as a respected assessment of capability to oversee an enterprise's information security.

- *Certified in Risk and Information Systems Control* (CRISC). The CRISC certification assesses capability in risk management, including risk assessment, response and monitoring.

International Information Systems Security Certification Consortium (ISC_2)

The ISC_2 [21] is a US-based international certification body which has been operating for over 20 years. Membership is related to certification.

By far the most influential of the ISC_2 certifications is the 'Certified Information Systems Security Professional' (CISSP). Indeed CISSP has become something of a global benchmark qualification in cyber security. CISSP certification requires passing an examination across ten domains of knowledge. It also requires evidence of at least 5 years of relevant work experience, although 1 year of credit is given for possessing certain academic qualifications (including a Master's degree in Information Security). Evidence of continued professional development is required to remain 'in good standing', otherwise the examination must be retaken every 3 years. CISSP holders can achieve further specialised certification in security architecture, security engineering and security management. $(ISC)_2$ also issues several other less prominent certifications in more specialist areas:

- Certified Secure Software Lifecycle Professional.
- Certified Authorization Professional.
- Systems Security Certified Practitioner.
- Certified Cyber Forensics Professional.
- HealthCare Information Security and Privacy Practitioner.

Commercial Qualifications

A third source of cyber security upskilling programmes is the private sector. There are far too many private providers for a comprehensive overview to be provided here. Common sense should be applied when considering commercial providers and care should be taken to research the reputation and quality before signing up to private offerings. There are many good suppliers, and some less good.

The SANS Institute

The 'SANS Institute' [22] merits special mention as it is one of the most significant suppliers of commercial training in cyber security. The SANS Institute is a private US company founded in 1989 and has gained an impressive reputation for the range and
scale of its training activities in cyber security. Many SANS courses are focused on specific security operations activities. There are more generic or foundation courses along with courses which highlight security aspects of other disciplines such as programming/ developing systems. SANS runs both long courses (focused on a specific role) and short courses (focused on specific skills within a role). SANS courses are available in a number of different delivery modes, including distance learning.

SANS has sufficient traction in this area that its activities stray into both the professional body and academic space:

- SANS runs the 'Global Information Assurance Certification' scheme which certifies information security professionals in both technical and practical aspects of cyber security.

- SANS operates the 'SANS Technology Institute', which is a private institution issuing Master's degrees (in information security management and information security engineering) and certificate programmes.

Vendor courses

Upskilling courses, such as those run by SANS are intended to be vendor-neutral. However, cyber security technologies are often complex and it is entirely appropriate that a number of vendors offer cyber security upskilling programmes based on their specific technologies. Several of these vendors are so ubiquitous in the marketplace that their technology-specific certifications can be very useful to obtain.

One well-known example of a vendor providing its own security certifications is Cisco. Security-related certification provided by Cisco [23] include (among others):

- *Cisco Certified Network Associate Security*, which validates the ability to set up a basic security network infrastructure, including core security technologies and monitoring.

- *Cisco Certified Network Professional Security*, which validates the skills to be a network security engineer, including maintenance and deployment of appropriate tools for routing, switching and security defence.

CESG Certified Training

As previously mentioned, one of the initiatives that forms part of the UK National Cyber Security Programme is the development of the CCT scheme [6]. The CCT scheme is intended to identify high standard cyber security training amidst the plethora of offerings on the market. An upskilling programme needs to have been rigorously assessed in terms of its content, trainers and ability to manage training events in order to qualify for CCT status. The CCT scheme is based on the IISP Skills Framework and over a dozen programmes are now CCT certified, with this number expected to grow.

Other Professional Development Activities

There are many other initiatives in the areas of cyber security training that do not fall neatly into the previous categories. A few of these are worth mentioning in order to give a flavour of the types of activity available.

The ‘Cyber Security Apprenticeship scheme’ is being run by the Tech Partnership [24] and provides on-the job training as well as some classroom-based training. This scheme is intended to accelerate new entrants into the cyber security profession by giving them real experience of working in the cyber security sector. The Tech Partnership is also supporting the development of ‘Cyber Academy Learning Pathways’, which are intended to align with the IISP Skills Framework and provide assistance for individuals planning career progression in cyber security.

The ‘Cyber Security Challenge’ [25] is an innovative series of national competitions designed to inspire people to enter the cyber security profession. While not directly a training activity, the Cyber Security Challenge does identify and inspire individuals to progress their cyber security skills, both as participants and as challenge setters. The Challenge also supports a cyber-security mentoring scheme.

There are a number of initiatives designed to support cyber security in specific sectors or targeting particular audiences. One example of the latter is ‘Responsible for Information’ [26], which is a free online course that has been developed by the UK Government for small and medium-sized enterprises to provide basic information security training.

Conclusion

There probably has never been a more interesting time to consider a career in cyber security. However, cyber security is both multi-faceted and constantly evolving, making it challenging to acquire and maintain the skills necessary to act as a responsible cyber security professional. Anyone aspiring to enter the cyber security profession would be wise to engage in some level of education and training, and perhaps seek to acquire suitable qualifications. Indeed, most people already employed as cyber security professionals regularly require upskilling. This article has reviewed a range of available options for cyber security education, qualifications and training. The main differences between available programmes have been identified and some guidelines on how to match personal needs to upskilling options have been discussed. It is hoped that these observations are of some assistance in charting a successful and rewarding career in the cyber security profession.

Acknowledgments

Thanks are due to Paul Dorey, Ian McKinnon and Fred Piper for useful conversations in preparation of this article.

REFERENCES

[1] 'Competitive analysis of the UK cyber security sector: A study by Pierre Audoin Consultants for the Department for Business, Innovation and Skills', Version 1, 29 July 2013, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/259500/bis-13-1231-competitiveanalysis-of-the-uk-cyber-security-sector.pdf, accessed March 2015

[2] 'Cyber Security Skills: Business Perspectives and Government's Next Steps, HM Government', March 2014, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/289806/bis-14-647-cyber-securityskills-business-perspectives-and-governments-next-steps.pdf, accessed March 2015

[3] 'The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world', HM Government, November 2011, https://www.gov.uk/government/publications/cybersecurity-strategy, accessed March 2015

[4] 'The Institute of Information Security Professionals', https://www.iisp.org

[5] 'IISP Information Security Skills Framework Version 6.1', IISP (2010), https://www.iisp.org/imis15/iisp/Accreditation/Our_Skills_Framework/iispv2/Accreditation/Our_Skills_Framework.aspx?hkey=e77a6f03-9498-423eaa7b-585381290ec4, accessed March 2015

[6] 'CESG Certified Training', http://www.cesg.gov.uk/awarenesstraining/certified-training/, accessed March 2015

[7] 'GCHQ Certification of Master's degrees in Cyber Security' http://www.cesg.gov.uk/awarenesstraining/academia/Pages/Masters-Degrees.aspx, accessed March 2015

[8] Masadeh, M.: 'Training, education, development and learning:what is the difference?', Eur. Sci. J., 2012, 8, (10), pp. 62–68

[9] 'Academic Centres of Excellence in Cyber Security Research', http://www.cesg.gov.uk/awarenesstraining/academia/Pages/Academic-Centres.aspx, accessed March 2015

[10] Furnell, S.: 'Securing a Good Degree?'. IISP Pulse, Spring 2011, pp. 6–8

[11] 'Oxford Centre for Doctoral Training in Cyber Security', https://www.cybersecurity.ox.ac.uk/education/cdt

[12] 'Royal Holloway Centre for Doctoral Training in Cyber Security', https://www.cybersecurity.ox.ac.uk/education/cdt

[13] 'Why cyber security is a safe choice for a postgrad degree', The Guardian, 24 June 2014, http://www.theguardian.com/education/2014/jun/24/secure-a-cyber-career, accessed March 2015

[14] 'Cousera', https://www.coursera.org/

[15] 'Future Learn', https://www.futurelearn.com/

[16] 'BCS: The Chartered Institute for IT', http://www.bcs.org/

[17] 'Certified Professionals', http://www.cesg.gov.uk/awarenesstraining/certified-professionals/Pages/index.aspx, accessed March 2015

[18] 'CESG Listed Advisor Scheme', http://www.cesg.gov.uk/servicecatalogue/CLAS/, accessed March 2015

[19] 'CREST: Assurance in Information Security', http://www.crest-approved.org/

[20] 'ISACA: Trust in, and value from, information systems', https://www.isaca.org/

[21] '(ISC)2: Inspiring a Safe and Secure Cyber World', https://www.isc2.org/

[22] 'SANS', http://www.sans.org/

[23] 'CISCO Training & Certifications', http://www.cisco.com/web/learning/certifications/, accessed March 2015

[24] 'Tech Partnership: Skills for the digital economy', http://www.thetechpartnership.com

[25] 'Cyber Security Challenge UK', http://cybersecuritychallenge.org.uk/

[26] 'Responsible for Information for SMEs', http://www.nationalarchives.gov.uk/sme/, accessed March 2015