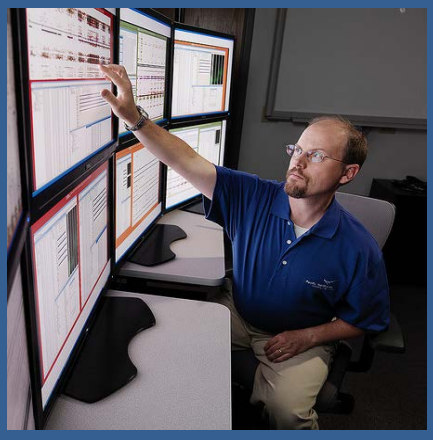
HM Government

Cyber Security Skills: a guide for business

Getting involved with skills and research initiatives



December 2014

Contents

Introduction

Purpose

1.1 This is an update of the cyber security skills guide for businesses originally published in March 2014. It is in response to calls from businesses for a clear listing of the *current* opportunities for them to engage with cyber security skills and research initiatives, particularly those that receive some public funding, such as through the £860m National Cyber Security Programme. Some of the initiatives are designed to benefit businesses and existing cyber security professionals directly, including ones that recognise professionalism and support its further development. Others provide opportunities to educate and inspire the pipeline of new talent vital to our future national security and prosperity, but all will benefit from the enthusiasm, insights and support businesses have to offer.

1.2 What are the benefits to your business of getting involved in initiatives to build cyber security skills?

- having the skills and capability to manage cyber risk effectively can reduce the financial cost to your business from cyber crime and increase consumer confidence;
- investment in new talent is both essential and cost effective - the demand for cyber security professionals, and the cost of securing them, is growing rapidly;
- it gives you influence over the skills, knowledge and experience that future cyber security professionals develop, ensuring they meet the needs of your business;
- you can help inspire a more diverse range of talented people to consider a cyber security career, increasing the quality and quantity of the talent pool; and
- it will increase awareness of the career opportunities you offer, and loyalty to your organisation, amongst those you most want to recruit and retain.

1.3 This guide will be periodically updated to ensure continuing currency and relevance.

Using this guide

1.4 The current initiatives businesses can both assist and benefit from have been grouped into three broad categories in this guide::

- **Initiatives supporting schools** – these include: helping shape attractive and relevant materials and classroom exercises for pupils to give them a deeper understanding of security concerns and industry practices; delivering competitions to encourage practical skills development; supporting the development of teaching expertise in cyber security; acting as valued STEM or other ‘ambassadors’ providing role models for young people and powerful insights into future learning and career possibilities.

- **Initiatives supporting vocational and higher education** – these include helping ensure that teaching and learning are informed by the real-life demands of cyber security work, through design and delivery of course content, providing work experience opportunities, mentoring students and developing ongoing relationships with teaching staff. There are also many opportunities to engage with cyber security research, to help ensure we build a vibrant research community, with good links to industry.

- **Initiatives supporting new or existing cyber security professionals** – these include schemes to recognise high quality training and education, and ways to help clarify professional entry and progression routes.

Executive Summary

Businesses and their staff have a diverse range of skills and research activities they can support and benefit from. Collectively, these activities cover school-level, through to vocational and higher education, and include activities focused on prospective and existing cyber security professionals. Some of the activities are funded wholly or in part through the Government's £860m National Cyber Security Programme; others include existing efforts to promote and recognise professionalism within the field of cyber security.

Businesses can: help ensure the development of the skills of the future cyber security workforce more closely match their needs; help attract a diverse range of new talent to their organisations and the cyber security sector more broadly, and invest in the development of the existing workforce.

'Cyber Security Skills: a guide for business' will help you choose which of the current range of skills and research initiatives best fit your interests, and signpost you directly to someone who will be happy to facilitate this.

The following summary outlines opportunities for businesses and individuals to get involved and benefit from doing so. Further details are given in the guide itself.

Initiative or activity	Opportunity to get involved	Page
Supporting schools		
Secure Futures campaign	Secure Futures is an employer-backed campaign delivered by the Tech Partnership which inspires young people to consider careers in cyber security. Employers can offer various forms of support, including offering volunteer ambassadors and help delivering workshop sessions in schools.	8
Behind the Screen	Behind the Screen is a computing curriculum development programme delivered by the Tech Partnership which includes cyber security teaching and learning materials for to pupils aged 11-18. Employers can get involved in the on-going development of these.	9
Cyber Security Challenge - schools programme	The Cyber Security Challenge offers a range of activities, teaching/learning resources and competitions to inspire young people about opportunities in the cyber security profession and help the development of practical cyber security skills. Employers can help further develop and deliver these.	10
STEM Ambassadors	STEMNET co-ordinates a range of ways for employees – including those with IT backgrounds – to volunteer to support schools in delivering activities that enrich education and provide inspirational role models.	11

Supporting vocational and higher education

Apprenticeships	Through the Tech Partnership, employers have created the first cyber security apprenticeships combining on the job learning, vocational training and academic education. Employers can recruit such apprentices, and volunteer to help future development work.	12
HE Internships	The Tech Partnership is supporting a scheme to match prospective interns to suitable paid work experience opportunities in the tech and cyber security fields. Employers can benefit by offering internships of flexible lengths to enthusiastic candidates.	13
Innovative teaching and learning	The HE Academy is supporting four projects involving employers partnering with academics to develop and showcase innovative resources and approaches to improve cyber security education at higher education institutions. Employers can engage with these, similar, and future projects via the HE Academy to help ensure HE teaching is more relevant to their needs.	14
Mentoring and cyber camps schemes	The Cyber Security Challenge will deliver two pilot schemes: a mentoring scheme and a series of cyber camps aimed at computer science students and recent graduates. Employers can offer volunteer mentors and practical support for the delivery of the camp skills activities.	15
Industry-backed degrees	The Tech Partnership has worked with employers to develop two IT degrees, both of which include cyber security learning outcomes and involve employers in their delivery, e.g. as guest lecturers and in shaping problem-based learning resources. Additional employers can get involved with such delivery and with any ongoing development of these and similar degrees.	16
Academic Centres of Excellence in Cyber Security Education	GCHQ is working with industry and academia to set standards for cyber security higher education, in the first instance certifying high-quality Masters degrees in the cyber security field. Employers can offer advice, help define and assure such standards, support curriculum development efforts, and sponsor students.	17
Academic Centres of Excellence in Cyber Security Research	GCHQ has led the recognition of 11 universities (so far) conducting internationally-leading cyber security research. Employers can fund research projects, support universities working towards such recognition and to exploit research, and assist with facilities to accelerate innovation.	18

Research Institutes (RIs)	Three Research Institutes (in the science of cyber security, automated program analysis and verification, and trustworthy industrial control systems) support collaboration between leading cyber security researchers. Employers can support these in various ways, including sponsoring forums to help disseminate findings and engaging with each RI to help ensure outputs are applicable to industry-relevant problems.	19
Centres for Doctoral Training (CDTs)	The CDTs located at Oxford University and Royal Holloway University of London are providing multidisciplinary training for the next generation of doctoral-level cyber security experts. Employers can collaborate with the CDTs to sponsor projects and help ensure the research meets their needs and real-world situations and problems.	20
Free online learning resources	A range of free online cyber security learning resources are available to increase basic cyber security awareness amongst the wider workforce, including an eight-week Open University 'Introduction to Cyber Security' course, a short information security course aimed at small and medium-sized businesses, and a tailored short course for legal and accountancy professionals. Employers can promote their use to staff and offer to help with future development work.	21

Supporting prospective or existing cyber professionals

Cyber Security Challenge – competitions	The Cyber Security Challenge organises national competitions to identify, inspire and enable more people to become cyber security professionals. Competitions allow safe environments for testing and demonstrating skills. Employers can sponsor and support such activities.	22
National skills standards and leaning pathways	The Tech Partnership has led the development of a single, coherent, set of skills standards for information security, and used these as the basis for developing 'learning pathways' towards entry into and progress through the cyber security profession. Employers can use the pathways to plan skills development within their organisations and help to refine them and develop new ones to meet their particular needs.	23
CREST - learning pathways and career development	CREST supports industry and career development through its Academic Partnership Programme, professional development, training and conferences, and production of 'day in the life' filmed interviews with practitioners. Employers can engage in numerous ways including becoming a CREST member company, encouraging uptake of CREST qualifications, and supporting development of careers resources to attract new talent into cyber security work.	24

CESG Certified Professional Scheme	GCHQ has established a certification scheme for cyber security professionals to recognise expertise across the public and private sectors, operated by three certifying bodies. Employers can encourage individuals to become certified or to support the certifying bodies as scheme assessors, and work with GCHQ to refine and extend the range of job roles covered.	25
CESG Certified Training Scheme	GCHQ has established a new certification scheme to provide assurance for cyber security training courses, with assessment by an approved certifying body. Employers can make use of the certified training and encourage training providers to seek certification.	26
CompTIA	CompTIA offers its Trustmark credential to cyber security solution providers. It also supports the Armed for IT careers programme for ex-forces personnel interested in starting a career in IT. Employers can seek to have their technical staff certified.	27
International Information Systems Security Certification Consortium (ISC)²	(ISC)² is a not-for-profit membership body of certified information and software security professionals. It produces resources to support communities, policy makers and the information security profession. Employers can seek to have their technical staff certified.	28

Please note the Tech Partnership is now taking forward the work of e-skills UK, including the e-skills UK activities described in this booklet. The Tech Partnership is a new network of employers collaborating to improve skills for the digital economy and encourage growth.

Initiatives supporting schools

Employer-backed Secure Futures campaign lifts the lid on cyber careers.

The opportunity to engage

Secure Futures is an employer-backed campaign, which forms part of the Cyber Academy's work to inspire young people to consider careers in cyber security. It offers schools bespoke workshops, delivered by cyber experts, and free follow-up teaching resources for Key Stages 3 and 4, including online games that simulate real life cyber situations. During the workshops, students learn about cyber threats and defences in cross-curricular contexts including classics, history, maths and art. Young people see that cyber security touches every part of their lives. The resources link the techniques young people can use to ensure their own online safety, with those used by government and business to protect the nation from cyber attack.

Secure Futures events have been held in universities, delivered in partnership with computing departments and Cyber Security Challenge. STEM ambassadors in the Manchester region have been trained to deliver Secure Futures sessions in local schools, using their personal experience of working in tech to bring the resources to life.

Employers can support Secure Futures in a variety of ways. Cyber security professionals can volunteer as ambassadors, visiting schools to deliver workshops in lessons or assemblies. They can also provide real world problems and inspirational role models to form part of the online teaching resources.

Benefits to employers

Since Secure Futures launched in September 2013, over 2,000 students in schools have said that they've been inspired about cyber security careers through the resources available. This is helping build a long-term pipeline of new entrants into the sector, with collaborating employers being particularly visible and well-positioned to benefit.

"Employer outreach to schools is one of the ways that the tech sector is helping to develop a sustainable skills pipeline that will ensure the UK's future as a global leader in cyber security." – Mark Smyth-Roberts, Business Director, C3IA Solutions Limited.

Contact

Rhian Kavanagh, the Tech Partnership

rhian.kavanagh@e-skills.com

www.bigambition.co.uk/secure-futures

TECH PARTNERSHIP

Behind the Screen puts industry-backed cyber content on the computing curriculum

The opportunity to engage

Through Behind the Screen – a computing curriculum development programme – employers are transforming what students learn in school. It forms part of the Cyber Academy's work to inspire young people to consider careers in cyber security.

Content on cyber security for Key Stage 4, developed by e-skills UK with input from BP, BT, CREST, Fujitsu, PwC and QinetiQ, has been taken up by over 450 schools. This project introduces core principles such as threat awareness and planning; cyber crime and computer forensics; security practices and principles; safety, privacy and ethics; and online interaction.

Similar resources were launched at the beginning of 2014 for Key Stage 5 students – those studying A level or level 3 vocational courses – and focus much more on real life cyber attack: its causes, effects, aftermath and recovery. Students explore the history of cyber security, including the geopolitical changes of the last decade, on an interactive timeline. They also take the role of cyber security professionals to model threats assess risks, identify and prioritise information assets. Over 30 cyber security employers supported the development of these resources, and will continue to do so, as more materials are created for Key Stage 3 students and for teachers. This is a new programme that aims to provide a 'cyber aware' accreditation pathway for individual teaching staff and institutions.

Employers can support Behind the Screen by becoming involved in the development of these new materials for young learners and teachers, as well as in a teacher mentoring scheme that is being launched later this year. Such inputs will help ensure greater priority is placed on effective cyber security education that is not limited to learning about online safety.

Benefits to employers

The authentic nature of the work carried out so far demonstrates that students appreciate the input of sector employers to bring alive the real life issues around cyber attack and its prevention. Such support can only foster more interest among young people, and contribute to a robust long-term pipeline of new entrants. The raised profile of collaborating businesses means they are particularly well placed to benefit reputationally, and to influence and support learning in schools actively and practically.

Contact

Sue Nieland, the Tech Partnership

sue.nieland@e-skills.com

www.behindthescreen.org.uk

TECH PARTNERSHIP

Cyber Security Challenge - schools programme

The opportunity to engage

The Challenge offers through its schools programme various fun, exciting and accessible activities that help younger audiences discover why cyber security matters and inspire them to want to defend the UK online.

In addition to organising cyber security competition activities aimed at young people, it also offers teaching resources which enable schools to quickly and easily encourage the exhibition of practical skills that are relevant to job roles in cyber security. These resources include kits explaining how to crack pre-prepared codes, and lesson plans with exercises that help students build their own ciphers.

These ciphers are then posted online for other schools to decipher. The schools which are most successful in cracking these ciphers qualify for a face-to-face Cyber Games final: a fun day of solving industry-set challenges.

A range of sponsors helped in developing these teaching resources.

Businesses can support the Challenge to further develop the range, relevance and attractiveness of educational resources, and possibly help with delivery.

Benefits to employers

Businesses supporting the Challenge's schools programme will have a raised profile amongst school pupils and be better-placed to influence the early career thinking of potential new young cyber security talent and those advising this group.

Contact

The Cyber Security Challenge

queries@cybersecuritychallenge.org.uk

www.cybersecuritychallenge.org.uk

Employers encouraging employees to become STEM Ambassadors

The opportunity to engage

Employers are encouraging their staff to volunteer as STEM Ambassadors – role models who inspire and support young people across the UK in understanding the relevance of science, technology, engineering and maths (STEM) skills in their lives, and the opportunities that studying these subjects can lead to.

There are over 28,000 STEM Ambassadors across the UK, of whom around 5,000 have a background in the IT, computing or digital sectors. At present, fewer than 100 have a background in cyber security. STEM Ambassadors carry out over 20,000 activities each year, in both primary and secondary schools.

The STEM Ambassadors Programme is nationally coordinated by STEMNET, with the support of the Department of Business, Innovation and Skills. STEMNET provides STEM Ambassadors with induction training, a free Disclosure and Barring Service check (or Protection of Vulnerable Groups check in Scotland), and on-going support throughout their time as volunteers including links with schools. STEM Ambassadors are asked to take part in one activity each year, though many choose to do more.

STEMNET works with many thousands of employers, and can tailor delivery of the programme to suit your strategic and operational needs.

Benefits to employers

Employers who are involved with STEMNET's programmes find opportunities to:

- Challenge stereotypes about the career paths of people with STEM skills and encourage new recruits
- Develop young peoples' skills, knowledge and understanding of STEM applications in the real world
- Contribute ideas to teachers about topics and activities to include in the STEM curriculum
- Tap into the creative thinking of young people
- Enhance the reputation of their company in the local community
- Provide career development opportunities for their employees by developing the communication, planning and presentation skills of STEM Ambassadors

Encouraging staff to become STEM Ambassadors means employers can slot into an existing framework that is both comprehensive and flexible. The programme is well-established and recognised by schools across the UK – 90% of secondary schools have worked with a STEM Ambassador in the last twelve months – and the demand from teachers with cyber security expertise is strong.

Contact

Kat Sandford, National STEM Ambassadors Programme Manager

kat.sandford@stemnet.org.uk

www.stemnet.org.uk/employers

STEMNET

Initiatives supporting vocational and higher education

Employers come together to develop cyber security apprenticeships

The opportunity to engage

Through the Tech Partnership, employers have created the first ever apprenticeship frameworks in cyber security. This has already created nearly 200 new entry-level jobs with more in the pipeline. Employers including Atos, Bango, the Cabinet Office, Capgemini, CGI, Jeffries Investment Bank and Steria have recruited new cyber security apprentices for the first time:

> *"We at CGI are really looking forward taking our first ever cyber security apprentices this autumn. It is a key component of our continued cyber security focus and will provide outstanding opportunities for young people to enter an exciting career!"* *(Verner Parke, Security Practice Lead, CGI)*

Employers can recruit these apprentices at two levels – advanced (for people with good GCSEs) and higher (for people with good A levels). 7 training providers either have or are developing courses to deliver the training element of the apprenticeship and two of them, QA and TDM, have already been licensed by the Tech Partnership as Tech Industry Gold for the outstanding quality of their cyber security apprenticeship training provision. The Partnership is now in discussion with other providers seeking Tech Industry Gold accreditation.

In addition, the Tech Partnership has developed a new Cyber Intrusion Analyst Trailblazer Apprenticeship, providing training in this specialised and strategically important role. The first vacancies are expected in September / October 2015 and the employer group which created the specification for the apprenticeship is now in discussion with a number of universities to quality-assure the programme. The training provided must be rigorous and must include a robust assessment process to demonstrate that apprentices completing the programme are fully competent in the role.

Benefits to employers

Recruiting apprentices has many benefits: making the workplace more productive; protecting against future skills shortages; introducing new ideas; reducing recruitment costs, and improving staff retention. There is also a significant government contribution to training costs. With Tech Industry Gold training, employers can be confident in the quality of the training and in apprentices becoming productive as quickly as possible:

> *"Employers like Visa Europe want to be confident that the apprenticeship we deliver is of an outstanding quality. Where a training provider's programme has been accredited as Tech Industry Gold, we can have that confidence. We at Visa Europe are likely to choose accredited programmes over non-accredited ones because we know they have been designed by employers for employers and the training delivery has been quality assured."* *(James Lawrence, Senior Talent Manager, Visa Europe)*

Contact

Mark Heholt, the Tech Partnership

mark.heholt@e-skills.com

www.e-skills.com/apprenticeships

TECH PARTNERSHIP

Cyber security employers come together to offer paid HE internships

The opportunity to engage

As part of the Tech Partnership Cyber Academy's work to provide new entry routes for young people into the sector, employers are coming together to offer paid HE internships. This will give more students the real world experience that is needed to enter the sector today.

The internships will be between 2 and 12 months in duration, and suitable either for undergraduates taking IT-related degrees, or for recent graduates. To make the most of internships, employers must have meaningful work for an intern to do; be willing to provide support such as a line manager or mentor; and pay them a fair rate.

The Tech Partnership is supporting employers by offering to advertise vacancies to suitably qualified students and process applications for free. The new internships are supported by CREST, IET, IISP AND (ISC)^2, and build on the summer 2013 BIS-sponsored internship pilot by IAAC.

Benefits to employers

By providing internships, cyber security employers can help shape the skill of future cyber security professionals. They can also get a head start in recruiting the most motivated students - internships are like a 2 to 12 month interview - and bring enthusiasm and a fresh approach to their business. An intern can be a cost effective way to add additional resource to a team.

"[Internships are] effectively an opportunity to interview a potential candidate for an extended period of time and know that if you do go on to recruit them, they'll already be up-to-speed with your business." - Charles White, CEO, IRM Plc.

Contact

Howard Skidmore, the Tech Partnership

Howard.Skidmore@e-skills.com

www.e-skills.com/offercyberinternship

TECH PARTNERSHIP

Innovative approaches to teaching Cyber Security in partnership with employers

The opportunity to engage

In August 2014 the Higher Education Academy (HEA) and the Department for Business, Innovation & Skills (BIS) announced the availability of Cyber Security teaching development grants of up to £40,000 for higher education providers in the UK, to improve and showcase cyber security teaching and learning. 4 grants have since been allocated to support innovative projects, each benefiting from partnership with industry, with projects beginning November 2014.

It is widely recognised that there needs to be closer working between academia and business to make educators for all Computing courses aware of developments in cyber security and to ensure that degree courses (undergraduate and postgraduate) meet business needs. These 4 grants offer the opportunity for industry to collaborate with academia in course design and delivery; influence innovative methods of course delivery; potentially offer entry-level professional qualifications in partnership; offer student sponsorship, internships and work experience and raise the profile of cyber security learning and teaching.

The four grant recipients are:

- Newcastle College – this project will develop an innovative approach to the active learning of cyber security, breaking down perceived barriers between current industrial practice and academic learning;
- Birmingham City University and Queen Mary University of London will work with an expert practitioner to develop scenario-based legal and digital forensics education reflecting real case studies to promote learner engagement and critical thinking;
- Edge Hill University will create online problem based learning scenarios and resources, and a knowledge exchange model of disseminating good security practice to SMEs via MSc placements;
- Liverpool John Moores University will provide a cloud-based training platform for practicing scenario-based challenges e.g. in vulnerability analysis, penetration testing and secure software development.

Benefits to employers

If the UK is to be equipped to respond to cyber threats, and the cyber security sector is to grow, we need to strengthen the pipeline of cyber talent and help prepare students for entry-level security career opportunities. This a specific opportunity for industry to work with academia, to bring an innovative and exciting approach to teaching cyber security skills and to help create learning materials such as on developing safe and secure software.

Contact

Karen Fraser, HE Academy

karen.fraser@heacademy.ac.uk

www.heacademy.ac.uk/funding-call/learning-and-teaching-cyber-security

The Higher Education Academy

Mentoring scheme and cyber camps help graduates and students bridge into cyber careers

The opportunity to engage

Some graduates lack the practical experience and a range of business, communication and technical skills to be amongst the strongest candidates for jobs, whatever else they have to offer.

Alongside a range of measures to enhance the employability of computing graduates, the Government is funding the Cyber Security Challenge to work with businesses to deliver two pilot schemes - a cyber security mentoring scheme and a series of 'cyber camps' to strengthen the skills of participating students and recent graduates from computing and other appropriate disciplines while promoting career opportunities in the businesses involved and the wider cyber security profession. The Cyber Security Challenge already has a great track record in promoting the profession and in preparing prospective job candidates for a career, through its competitions, masterclasses and careers advice

Mentoring scheme

Under the mentoring scheme, volunteering employees from the cyber security profession will act as mentors for recent graduates and students interested in a cyber security career. The mentoring support might include advice about cyber roles, skills requirements and training opportunities, help with CVs and interview preparation, work shadowing or a short placement.

Cyber Camps

The cyber camps will be delivered in association with universities and will offer the participants hands-on experience of cyber security over several days, and the opportunity to gain an industry-recognised foundation qualification in the subject. The exercises will help develop communication and business skills as well as technical skills. Businesses might offer endorsement and practical support in a variety of ways that suits them (e.g. involvement in setting/running exercises, presenting to participants about career opportunities, providing refreshments/venues).

Benefits to employers

Both schemes will increase the positive profile of the company and the career opportunities it offers, provide exposure to potential recruits (with strengthened skills and experience) and provide an excellent development opportunity for employees who get involved. The projects will also help to build links between businesses and universities, and promote cyber security as a socially responsible profession that invests in new talent.

Contact

Debbie Tunstall, Universities Programme Manager

dtunstall@cybersecuritychallenge.org.uk

www.cybersecuritychallenge.org.uk

Employers make cyber security an integral part of industry-backed degrees

The opportunity to engage

Employers are ensuring that cyber security is an integral part of the curriculum for the industry-backed degrees from the Tech Partnership, as part of the Cyber Academy's work to provide new entry routes for young people into the sector.

The IT Management for Business (ITMB) undergraduate degree is supported by over 90 companies and available at 18 universities. A postgraduate version is being piloted at University of Exeter with 3 universities negotiating to offer in 2015. Security risks are now included in its learning outcomes. Employers such as Deloitte have delivered guru lectures and set challenges for students based on real-world security scenarios.

The Software Development for Business degree has been designed by employers including the BBC, BT, Cisco, Intel and Accenture. 9 universities will offer it from 2014 and 2015. Software security is a key element of the programme, covering risks, threats, testing and secure architecture. Students will also benefit from guru lectures, plus employer presentations and case studies to keep abreast of advances in the field.

Universities across the country are keen to receive offers of support from employers to enrich teaching and learning, both for these 2 particular degrees but also more widely.

Benefits to employers

By supporting these industry-backed degrees, employers can get early access to promising technology graduates with the skills they want by engaging with potential recruits early in their degrees and potentially save on graduate recruitment costs. Collaboration will raise their profile as graduate employers and awareness of emerging recruitment opportunities.

"These degrees are a unique opportunity for us to shape the next generation's skills. Through direct collaboration with universities, SAS and other companies help to develop degree programmes to produce fit-for-work graduates." – Geoffrey Taylor, Academic Programme Manager, SAS Software.

Contact

itmb@e-skills.com

softwaredegree@e-skills.com

www.e-skills.com/education/e-skills-degrees

TECH PARTNERSHIP

Academic Centres of Excellence in Cyber Security Education

The opportunity to engage

GCHQ, supported by BIS and Cabinet Office, is consulting extensively with academia and industry to set standards for cyber security education. Universities and courses assessed as meeting these standards will be the best in the UK.

GCHQ's initial focus is on identifying and certifying high quality Master's degrees in the cyber security field. Standards have already been written for:

- Master's degrees providing a foundation in general cyber security
- Master's degrees providing a foundation in digital forensics
- Master's degrees providing a foundation in network and internet security.

Organisations can continue to contribute by:

- helping to define specific types of Master's degrees that are needed
- providing evidence of specific skills requirements to help define the content of courses
- working with universities to embed industry recognised programmes into the curriculum where required
- helping to define and assure the standards against which the Master's degrees will be assessed
- committing to sponsor students to attend certified Master's degree courses
- advising on the set-up of the ACEs-CSE

It is likely that GCHQ will begin to consider the establishment of Academic Centres of Excellence in Cyber Security Education (ACEs-CSE) during 2015/16. Organisations are welcome to advise on the standards against which applicants will be assessed.

Benefits to employers

Promoting GCHQ-certified Master's degrees in the workplace will ensure that the investment made by the student and employer in the Master's degree is worthwhile.

Certified Masters in General Cyber Security

www.cesg.gov.uk/awarenesstraining/academia/Pages/Masters-Degrees.aspx

Academic Centres of Excellence in Cyber Security Research

The opportunity to engage

Eleven universities so far have been recognised as Academic Centres of Excellence in Cyber Security Research (ACEs-CSR). The initiative is sponsored by GCHQ, Research Councils UK, BIS, Cabinet Office and CPNI.

The ACEs-CSR have been assessed as conducting internationally-leading cyber security research and this recognition will:

- enhance the quality and scale of academic cyber security research and postgraduate training being undertaken in the UK
- make it easier for potential users of research to identify the best cyber security research and postgraduate training that the UK has to offer
- help to develop a shared vision and aims among the UK cyber security research community, inside and outside academia

Businesses can:

- Fund additional research projects within an ACE-CSR
- Support universities working towards recognition as an ACE-CSR
- Help universities maximise the opportunities from ACE-CSR recognition, working with universities to capitalise upon and exploit research
- Donate or fund university facilities to accelerate innovation
- Support two-way secondments between industry and academia

Benefits to employers

Businesses actively engaged will be well-placed to benefit from prompt exploitation of high quality research into cyber security and, over time, to build further beneficial collaborations with higher education researchers.

Academic Centres of Excellence in Cyber Security Research

www.cesg.gov.uk/awarenesstraining/academia/Pages/Academic-Centres.aspx

A brochure detailing the work of the ACE-CSRs can be downloaded here:

www.gov.uk/government/publications/cyber-security-research-capability-academic-centres-of-excellence

Research Institutes in Cyber Security

The opportunity to engage

Research Institutes in Cyber Security are virtual entities facilitating collaboration between leading researchers.

The first GCHQ-EPSRC sponsored Research Institute in Science of Cyber Security is a virtual institute comprising six universities under the directorship of Professor Angela Sasse of UCL. The 3.5 year programme focuses on understanding the overall security of organisations, including their constituent people, processes and technology to answer two key challenge areas:

- How secure is my enterprise?
- How do we make better security decisions?

The GCHQ-EPSRC sponsored Research Institute in Automated Program Analysis and Verification is directed by Professor Philippa Gardner of Imperial College London. The three year programme focuses on undertaking internationally-leading research which provides the foundation for the development of new methodologies and research-quality tools and techniques which can be applied to post-development programs. The six projects address the challenge areas of:

- vulnerability discovery
- malware analysis and classification of code
- improved defences and mitigations

The CPNI-EPSRC funded Research Institute in Trustworthy Industrial Control Systems is directed by Professor Chris Hankin of Imperial College London. Its five projects will run for three years and focus on understanding the risks to and securing the industrial control systems which oversee the correct functioning of parts of the UK's critical national infrastructure.

Organisations can contribute by offering to provide or sponsor a forum for the Research Institutes to disseminate and discuss their findings.

Benefits to employers:

Providing sponsorship and other support and engaging with the Research Institutes will enable ideas and techniques from the academic domain to be applied to industrially relevant problems in cyber security.

Contact

Contact the Directors or visit:

www.riscs.org.uk or

https://verificationinstitute.org

Cyber Security Centres for Doctoral Training (CDTs)

Opportunity to engage

The Cyber Security Centres for Doctoral Training (CDTs) located at **Oxford University** and **Royal Holloway, University of London** deliver multidisciplinary training that provides the skills needed by the UK's next generation of doctoral-level cyber security experts. In doing this, centres are engaging with businesses to ensure this training reflects the complex and dynamic nature of cyber threats. Training lasts for four years and comprises a formal assessable programme of taught courses (equivalent to Masters-level) in a range of subjects addressing key areas of cyber security, together with a related challenging and original research project. The centres will between them produce at least 78 graduates who will have the ability to contribute research-derived expertise to business or Government.

Oxford University

The Oxford University CDT focuses on emerging technology themes and cover pressing cyber security challenges such as: security of ‘Big Data’, cyber-physical security, effective systems verification and assurance and real-time security.

Royal Holloway, University of London

The Royal Holloway CDT focuses on problems faced by businesses and government such as: the design and analysis of cryptographic algorithms and protocols, the design of security services for embedded systems, telecommunications networks and critical infrastructure, the detection and analysis of malware, and the study of economics, psychology and sociology in the context of cyber security.

Benefits to employers

By working closely with CDTs and sponsoring projects, businesses are able to collaborate and work with universities on research that can help solve their needs.

Businesses will also be able to access expertise and awareness of new trends and ideas as they develop. Students will receive training that reflects real-world problems making the graduates more attractive as potential recruits and businesses will have access to well-qualified graduates for their workforce.

Contact

Maureen York, University of Oxford

cdt@cybersecurity.ox.ac.uk

www2.cybersecurity.ox.ac.uk/cdt

Contact

Prof Carlos Cid, Director, RHUL

cybersecuritycdt@rhul.ac.uk

www.royalholloway.ac.uk/isg/cybersecuritycdt

Cyber security free online learning resources: introductory level

The opportunity to engage

A range of free online learning packages have been produced with Government support, offering learning opportunities accessible to a wide range of people with a potential interest in cyber security:

'Introduction to Cyber Security MOOC' (massive, open online course) – will improve cyber security knowledge and awareness through introducing learners to basic cyber security concepts. This certified training course offers an eight week learning opportunity starting at several times during the year which can be taken at a learner's convenience. It covers different types of malware and concepts such as network security, cryptography, risk management and the threat landscape. There are no pre-existing requirements to enrolling on the course, and no previous knowledge is assumed. The course will run across 2015 (January 26th, April 20th, July 27th, and October 12th 2015) with the 2016 run scheduled for January 18th 2016.

biscybersecurity@bis.gsi.gov.uk

www.futurelearn.com/courses/introduction-to-cyber-security

'Responsible for Information' for SMEs – a free e-learning course aimed at staff in micro, small and medium-sized enterprises (SMEs). It helps employees and business owners to understand information security and associated risks, and it provides good practice examples and an introduction to protection against fraud and cyber-crime. The course is divided into three modules: General user, Information Asset and Information Risk Owners, Directors and Business Owners. Each module is tailored to the specific needs of the target audience and includes role-specific content.

IATraining@nationalarchives.gsi.gov.uk

www.nationalarchives.gov.uk/sme

'Cyber Security for Legal and Accountancy Professionals' - a free 4-module course designed for lawyers and accountants developed with the support of the Law Society and ICAEW, helping such trusted professionals understand what cyber security is and how it affects both them and their clients.

Available via the Law Society's CPD website

http://cpdcentre.lawsociety.org.uk/course/6707/cyber-security-for-legal-and-accountancy-professionals

Benefits to employers

These interactive materials enable you to equip employees across your organisation with basic awareness and knowledge of cyber security, helping to protect the information assets of your organisation, clients and consumers.

Initiatives supporting prospective or existing cyber security professionals

Cyber Security Challenge - Competitions

The opportunity to engage

The Cyber Security Challenge is a series of national competitions, learning programmes, and networking initiatives designed to identify, inspire and enable more EU citizens resident in the UK to become cyber security professionals.

Established to bolster the national pool of cyber skills, it offers a unique programme of activities to introduce sufficient numbers of appropriately skilled individuals to learning and career opportunities in the profession.

The Challenge is already helping to find hidden talent across the nation. It provides safe environments in which thousands of people can test and demonstrating their skills; and showcases the spread of opportunities for future cyber defenders.

It acts as a catalyst for:

- Identifying those with appropriate skills
- Inspiring them to seek learning opportunities and a career in cyber security
- Informing them about available education and training opportunities
- Enabling them through the awarding of prizes as training courses

Benefits to employers

The Challenge acts as a gateway to addressing the cyber security objectives in many business areas for our sponsors, including recruitment, brand awareness and PR, and the opportunity to network in a non-competitive environment with like-minded organisations facing similar challenges and opportunities.

Contact

The Cyber Security Challenge

queries@cybersecuritychallenge.org.uk

www.cybersecuritychallenge.org.uk

CREST supports learning pathways and career development

The opportunity to engage

There is an acute shortage of skilled individuals in the technical information assurance community. CREST supports industry and career development through its Academic Partnership Programme, professional development, training and conferences and production of 'Day in the Life' films, which together help create a profession with clearly laid-out career paths.

Day in the life films

Filmed interviews with people working in a wide range of different roles at all levels in the information assurance industry provide information on potential careers paths, as well as important advice, encouragement and information from those actually working in the roles. Over 60 films have now been produced and can be accessed at www.youtube.com/crestadvocate. The development of a virtual skills hub is also underway to provide a focal point for careers, education, training and employment opportunities.

Training Partners

CREST recognises the need for professional development programmes and works with others to develop learning pathways into the sector and assists training course providers with a defined structure to develop courses. CREST is also launching a Training Course Assessment Programme that will assesses the content of IA and cyber security courses against the framework for the CREST qualifications.

Academic Partners

CREST is working with academia as part of its Academic Partnership Programme. The aims of this Programme are to support relevant Universities to encourage the best people into the industry, develop real and tangible links with business and to provide real employment opportunities for graduates.

Student Membership

CREST Student membership offers inclusion in the CREST community to augment students' studies.

Industry Internships

Internships or work placements are a great opportunity for students to gain real world experience to complement their academic coursework, and CREST circulates the CV's of students available for internships or work placements to representatives from CREST Member companies.

Benefits to employers

CREST qualifications are the gold standard for technical information security and if member companies do not adhere to audited policies, processes and procedures they can be removed from the register. Becoming a CREST member company helps to demonstrate both the company's professionalism and the professionalism of the industry as a whole. Existing Information security professionals can help grow the reputation of the industry as a career path by augmenting their existing skills with CREST qualifications.

Further details on CREST activities and how you can work with CREST to make the information technology world a safer place can be found on the CREST website.

Contact

Elaine Luck, CREST

elaine.luck@crest-approved.org

www.crest-approved.org

Employers create unified national skills standards and learning pathways for cyber security

Opportunity to engage

As part of the Cyber Academy's work to improve access to relevant, high quality training, industry has come together through the Tech Partnership to create a single, coherent, national set of skills standards for information security.

These are forming the basis for new learning pathways, to help identify the skills and work experience needed to enter and excel in the cyber profession.

The new standards combine the employer-backed e-skills UK IT Professional Standards (ITPS) with GCHQ's supplemental skills statements supporting the CESG Certified Professional (CCP) scheme. Both are being aligned to the Institute of Information Security Professionals (IISP) Information Security Skills Framework. The new standards offer one common language that professionals, public and private sector employers, and training providers can all use to benchmark information security skills.
Providing the building blocks for job roles as well as qualifications and training programmes, the standards help industry identify skills gaps, and define new learning and career pathways to fill them.

Benefits to employers

Employers can use ready-made learning pathways to plan skills development for their organisation.

Employers can also "adopt a pathway" – working with e-skills UK, to define pathways and keep them relevant, or build new pathways to meet their own particular skills needs and organisational structure.

Through their involvement in developing the new standards and pathways, employers have ensured that the design will maximise utility and relevance for particular businesses and circumstances. Using existing pathways gives employers, in one place, training options available to help an individual perform in a job and achieve a range of qualifications, exams and accreditations.

Contact

Nigel Payne, the Tech Partnership

nigel.payne@e-skills.com

TECH PARTNERSHIP

CESG Certified Professional (CCP) Scheme

Opportunity to engage

GCHQ has established a certification scheme for cyber security professionals known as CESG Certified Professional (CCP).

The CCP scheme recognises the expertise of those working in the Information Assurance and Cyber Security arenas in both government and industry. It sets the standard for IA professionals working in this sector and provides a rigorous and independent assessment of the competence of IA professionals.

The CCP scheme assesses candidates at levels of competence across 7) roles. The skills required to perform each Role are based on skills and skill framework developed by the Institute of Information Security Professionals (IISP) www.iisp.org and supplemented by CESG. The roles currently offered for certification are: Accreditor, Security and Information Risk Advisor, IA Architect, IA Auditor, IT Security Officer, Communications Security Officer and Penetration Tester.

CCP is not a qualification but a certificate of competence and aims to be a key foundation of an emerging cyber security profession. The scheme is operated on behalf of GCHQ by three certification bodies: APM Group, BCS and IISP (with Crest and RHUL). All applicants are required to prove UK residence.

Organisations can contribute to this initiative by:

- Encouraging employees to become certified through the scheme
- Working with GCHQ to refine existing roles and develop new ones that are applicable across the public/private sector
- Supporting the certification bodies by encouraging specialists to work as assessors
- Helping promote and embed the scheme by insisting cyber security specialist employees and those supplying organisations are CESG Certified Professionals

Benefits to employers

Employers supporting and promoting use of the scheme and its further development, will have the assurance that individuals with CCP in a specific role have been independently and rigorously assessed and have demonstrated their expertise in cyber security and their ability to apply relevant skills, knowledge and experience effectively within a business environment

Contact

CESG Certified Professional scheme

profcert@cesg.gsi.gov.uk

www.cesg.gov.uk/awarenesstraining/IA-Certification/Pages/index.aspx

CESG Certified Training Scheme

Opportunity to engage

GCHQ has established a new certification scheme for cyber security skills known as CESG Certified Training (CCT).

Training providers can submit their cyber security courses to a CESG-approved Certification Body (CB). The courses will be assessed by the CB against a CESG-approved standard which will measure both course content and delivery.
The basis for the scheme is to provide an assurance that training courses will offer cyber security skills at the level advertised – awareness or advanced – and by a trainer proficient in the subject matter and how to deliver it.

The training will be of interest to anyone seeking to advance their cyber security skills, including individuals aspiring to gain or enhance their professional status through the CESG Certified Professional (CCP) Scheme. Course content will be assessed against criteria consistent with the criteria used to assess the GCHQ Certified Cyber Security Master's degrees.

APM Group has been appointed as the Certification Body and details of certified courses can be found on their website.

Organisations can get involved by:

- Using the certified training courses to provide an uplift in Cyber Security skills for employees
- Encouraging providers of good Cyber Security training courses to submit these to the Certification Body for CESG certification
- Providing regular feedback on the quality of content and delivery of Certified Training courses to the Certification Body.

Benefits to employers

Participating employers can have confidence that specific courses certified under the scheme provide a good standard of training in cyber security content and delivery.

Contact

CESG Certified Training scheme

profcert@CESG.GSI.GOV.UK

http://www.cesg.gov.uk/awarenesstraining/certified-training/Pages/index.aspx

CompTIA - Is your IT team prepared to handle today's cyber threats?

The opportunity to engage

CompTIA is a vendor-neutral, non-profit IT association operating globally, with over 30 years of experience, around 2,000 member organisations, and 30,000 registered content users.

CompTIA invest in understanding the IT market. Its *11th Annual Information Security Trends Report* highlights that only 13% of organisations have made changes to their security approach over the last two years. To download the full report visit www.CompTIA.org/Register.

The CompTIA Security Trustmark is a business-level credential given to solution providers that consistently follow best practices in personnel security, security training and infrastructure. With a CompTIA Security Trustmark, companies can experience greater marketability and customer satisfaction. Customers can be confident their information is safe and secure. Find out more at www.comptia.org/trustmarks/security-trustmark

Armed for IT is a careers programme for ex-forces personnel interested in starting a career in IT. To learn more visit http://armedforitcareers.org/ Employers can show support for the initiative by joining a registry and commit to recruit ex-service personnel.

Benefits to employers

CompTIA can help businesses concerned about their IT Security. In a multi-device, multi-vendor connected world, employers can benefit from IT professionals who possess validated IT skills to keep their businesses ahead of the game. Once certified with essential skills in security, networking, mobility, cloud, storage, troubleshooting and project management your certified IT team will help transform your organisation.

Certifying technical staff can have a number of benefits:

- **Qualified Employees** - Certification is the best way for employees to demonstrate their competency and knowledge.
- **Hiring Tool** - To include certifications as a requirement in your job postings will increase the likelihood of recruiting the most capable personnel.
- **Stronger Workforce** - CompTIA gives businesses the tools for their employees to grow, including a broad range of certifications that help IT professionals validate their abilities.
- **Return on Investment** - A qualified IT department is a major component of a successful business. Certifications validate employee training programs, rewarding your investment with a skilled IT workforce.

http://certification.comptia.org/ExploreCareers/careerpaths/career_roadmap.aspx

Contact

Radhika Dattani

rdattani@comptia.org

www.comptia.org

CompTIA. The IT Industry Trade Association

International Information Systems Security Certification Consortium (ISC)²

Formed in 1989 and celebrating its 25th anniversary, (ISC)² is the largest not-for-profit membership body of certified information and software security professionals worldwide, with over 100,000 members in more than 160 countries, including more than 16,000 in the EMEA region and 5,000 in the United Kingdom. Globally recognised as the Gold Standard, (ISC)² issues the Certified Information Systems Security Professional (CISSP®) and related concentrations, as well as the Certified Secure Software Lifecycle Professional (CSSLP®), the Certified Cyber Forensics Professional (CCFP), Certified Authorization Professional (CAP®), HealthCare Information Security and Privacy Practitioner (HCISPP) and Systems Security Certified Practitioner (SSCP®) credentials to qualifying candidates.

(ISC)²'s certifications are among the first information technology credentials to meet the stringent requirements of ISO/IEC Standard 17024, a global benchmark for assessing and certifying personnel. (ISC)² also offers education programs and services based on its CBK®, a compendium of information and software security topics. More information is available at www.isc2.org.

The opportunity to engage

(ISC)^2 produces a range of resources and initiatives to support communities and policy makers as well as the information security profession. These are driven by the efforts of its advisory boards, local chapter network and the (ISC)² Foundation, an independent charity established in September 2011 to enhance cyber security education and awareness in the community. Initiatives include the (ISC)² Safe and Secure Online programme, a community service and engagement by (ISC)^2 members to secure vulnerable publics, a global scholarship programme and work to develop the next generation of information security professionals.

Publications include the (ISC)^2 Global Information Security Workforce Study, and related reports, conducted since 2004 by industry analysts to provide the only research-based resource of its kind tracking the growth of the workforce and the development of its profile.

Benefits to employers

(ISC)^2 certifications are based on the most comprehensive and widely accepted set of maintained best practices in the world, the (ISC)^2 CBK®. The CBK is a compendium of information security topics recognised and accepted by information security professionals and academic communities around the world, and kept up to date through regular member-wide job task analysis. The (ISC)² certification process requires members ensure their information security knowledge is continually updated by earning continuing professional education credit . Members work across all industry sectors and government.

Contact

Adrian Davis, (ISC)^2

adavis@isc2.org

www.isc2.org

This publication is also available on our website at www.bis.gov.uk

Any enquiries regarding this publication should be sent to:

Department for Business, Innovation and Skills
1 Victoria Street
London SW1H 0ET
Tel: 020 7215 5000
biscybersecurity@bis.gsi.gov.uk

If you require this publication in an alternative format, email enquiries@bis.gsi.gov.uk, or call 020 7215 5000.

BIS/14/1276