HM Government

Cyber Security Skills: a guide for business

Getting involved with skills, knowledge and capability initiatives

March 2014

Contents

Introduction

Purpose

1.1 This guide is in response to calls from businesses for a current and clear listing of the key opportunities for them to engage with cyber security skills and capability initiatives, particularly those that receive public funding. In some cases the initiatives were designed to benefit businesses and cyber security professional directly: in others the principal beneficiaries are the future 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 Widely publicising such opportunities has been an important part of developing and delivering skills and capability initiatives in support of the National Cyber Security Strategy. However, the diversity of such work has meant that more can always be done to inform or refresh businesses' appreciation of the breadth of opportunities for them to get involved and just as importantly how they might benefit in a rather more direct way from this.

1.3 Feedback from businesses consistently suggest that more organisations - and individuals employed by them - might be willing to support and so better benefit from the skills and capability initiatives if these were simply listed in one accessible place, with the type of opportunities to get involved transparent and not obscured by unnecessary detail. In some cases the benefits to business will be immediate, but in others their involvement will secure future and ongoing ones. This resource is a response to that call – a collation of the key features of such initiatives, suggesting what the key benefits to business would be in getting involved, and who to approach with any detailed follow-up questions or expressions of interest.

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

Using this guide

1.5 Most of the initiatives listed below are publicly-funded, either directly through the £860m 5-year National Cyber Security Programme or via support from the UK Commission for Employment and Skills (UKCES). UKCES-funded initiatives are often known through the 'Cyber Academy' brand of e-skills UK, but for the purposes of this resource it does not matter how the public funding is routed or branded, it matters more who to contact.

1.6 The various current initiatives businesses can both assist and benefit from have been grouped into 3 broad categories in the following Index section. This is to help the reader quickly pinpoint where their involvement will assist with secondary and tertiary education or with development of the cyber security profession, so yield longer- and shorter-term business benefits:

- Initiatives supporting schools;
- Initiatives supporting vocational and higher education;
- Initiatives supporting new or existing cyber security professionals.

Index

Initiatives supporting schools

Initiatives supporting vocational and higher education

Initiatives supporting new or existing cyber security professionals

Initiatives supporting schools

Employers inspire girls about cyber security through CC4G (Computer Clubs for Girls).

The opportunity to engage

The Cyber Academy's work to inspire young people to consider careers in cyber security includes employers supporting the industry-led Computer Clubs for Girls (CC4G), managed by e-skills UK.

Over 150,000 girls from more than 4,500 schools have now taken part in the online clubs, which encourage them to take on the digital world with confidence. CC4G's creative projects bring IT to life in contexts that girls can easily relate to. They include:

- Coding@CC4G**:** a unique set of learning materials that introduce girls aged 8 to 13 to the building blocks of code, created in partnership with UBS and the students of The Bridge Academy, Hackney;

- CC4G Power Up**:** an interactive learning resource focused on the role of technology within the main control room of National Grid. Girls get to see how it is used to manage and optimise the distribution of power, and fend off cyber attacks. Power Up is being developed in partnership with National Grid and will be launched in September 2014.

Employers can support CC4G in two main ways – sponsoring a school to run a club for a year, or working with CC4G to develop a new project based on their real world problems and role models.

Benefits to employers

Such employer support helps showcase the exciting opportunities available in technology and in their businesses to young women, showing a particular willingness to actively address the industry's gender imbalance (just 10% of those who hold technical roles in cyber are women). "Infosys is delighted to be sponsoring CC4G. Developing the IT talent pool is vital for the future of our sector and in supporting CC4G we're making sure that pool keeps growing." – Infosys.

Where can I find more details?

Contact Laura Cole at e-skills UK at laura.cole@e-skills.com or visit www.cc4g.net/sponsor-a-school-computer-club

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 free, dynamic teaching resources for Key Stages 3 and 4, including fun, online games designed to simulate real life cyber situations. These make the link between the techniques young people can use to ensure their own online safety, and those used by government and business to protect the nation from cyber threats.

Secure Futures is part of the IT sector's careers advice website BigAmbition, managed by e-skills UK. The work is being coordinated with other schools outreach activity from Cyber Security Challenge and STEM Ambassadors.

Employers can support Secure Futures in a variety of ways. Cyber security professionals can volunteer as ambassadors, visiting schools to deliver the materials in lessons or assemblies, and supplement the sessions run by teachers. 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 1,000 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.

Where can I find more details?

Contact Rhian Kavanagh at e-skills UK at rhian.kavanagh@e-skills.com or visit www.bigambition.co.uk/secure-futures

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 is already available and has been taken up by over 360 UK schools. This 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 for Key Stage 5 will be available from January 2014. Students will take on the role of cyber security professionals, to model threats, assess risks and prioritise assets, and handle a hacking scenario where a small business is targeted. Over 30 cyber security employers have supported the development of the Key Stage 5 resources, giving them the opportunity to ensure that what students learn at A-level is true-to-life and engaging.

Employers can support Behind the Screen further through mentoring in schools, and aiding the development of additional online resources aimed at teachers and Key Stage 3 students. Such inputs will help ensure greater priority is placed on effective cyber security education that is not limited to learning about online safely.

Benefits to employers

Such further support from business will foster interest among young people in the sector in general and help build 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 actively influence and practically support learning in schools.

Where can I find more details?

Contact Sue Nieland at e-skills UK at sue.nieland@e-skills.com or visit www.behindthescreen.org.uk.

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.

It also offers teaching resources that enable schools to quickly and easily encourage the exhibition of practical skills that are relevant to job roles in cyber security. These include kits explaining how to crack pre-prepared codes, and lesson plans with exercises that help students build their own ciphers. 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.

Where can I find more details?

Please contact queries@cybersecuritychallenge.org.uk

Initiatives supporting vocational and higher education

Cyber security employers come together to offer paid HE internships

The opportunity to engage

As part of the Cyber Academy's work to provide new entry routes for young people into the sector, employers are coming together to offer paid HE internships from summer 2014. This will give more students the real world experience that is needed to enter the sector today.

The internships will be between three and 12 months long, and suitable for either undergraduates taking IT-related degrees or postgraduates on specialist Masters courses. 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.

e-skills UK 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 skills of future cyber security professionals. They can also get a head start in recruiting the most motivated students - internships are like 3 or 12 month interview – and bring enthusiasm and a fresh approach to their business. An intern can be a cost-effective way to add an 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.

Where can I find more details?

Contact Howard Skidmore at e-skills UK at howard.skidmore@e-skills.com or visit www.e-skills.com/offercyberinternship

Employers come together to develop cyber security apprenticeships

The opportunity to engage

Employers, supported by e-skills UK, have developed new cyber security apprenticeships, as part of the Cyber Academy's work to provide new entry routes into the sector.

Those involved include Atos, BT, Cassidian, CREST, IBM and QinetiQ. Together, they have defined the learning outcomes that apprentices should attain, and e-skills UK has issued the frameworks that govern these.

Over 70 people have already started cyber security apprenticeships, and e-skills UK is working with high quality training providers to deliver more, with another 100 apprentices anticipated to start in the summer.

Employers can recruit these cyber security apprentices at two levels – advanced (for people with good GCSEs) and higher (for people with good A levels).

e-skills UK can provide help to ensure employers choose a training provider that can meet their skills needs and deliver the learning outcomes they require.

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.

Because the new cyber security apprenticeships have been designed by industry, employers can be sure that apprentices will gain the right skills.

Where can I find more details?

Contact Mark Heholt at e-skills UK at mark.heholt@e-skills.com or visit www.e-skills.com/apprenticeships

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 e-skills UK, 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) degree is supported by over 80 companies and available at 19 universities. 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 O2. 11 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 advancements 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.

Where can I find more details?

Contact itmb@e-skills.com or softwaredegree@e-skills.com, or visit www.e-skills.com/education/e-skills-degrees

Academic Centres of Excellence in Cyber Security Education

The opportunity to engage

GCHQ, supported by BIS and OCSIA is consulting extensively with academia and industry to define criteria which will help GCHQ and other employers to identify universities that are excellent in the cyber security education provided.

As a first step, GCHQ intends to identify high quality Masters courses through a new certification scheme focused specifically on cyber security. The Certified Masters in General Cyber Security is scheduled to launch 2014/15.

Organisations can contribute by:

- helping to define specific types of Masters courses that are needed;
- providing evidence of specific skills requirements to help define the content of courses;
- working with universities and course vendors to embed industry recognised programmes into the curriculum where required;
- helping to define and assure the standards against which the Masters will be assessed;
- committing to sponsor students to attend certified Masters courses;
- advising on the set-up of the ACE-CSE scheme.

Benefits to employers

Participation in scheme design will help ensure the outcomes are of relevance to employers' recruitment needs. Working with universities will strengthen business links with particular HE programmes and academics and open up further opportunities to collaborate. Supporting individual students will give employers more control over learning and better access to talented recruits.

Where can I find more details?

Further details on Certified Masters in General Cyber Security may be obtained by emailing academia@gchq.gsi.gov.uk

Academic Centres of Excellence in Cyber Security Research

The opportunity to engage

Eleven universities have been recognised by GCHQ as ACE-CSRs. The initiative is sponsored by BIS, the Centre for the Protection of National Infrastructure (CPNI), GCHQ, the Office of Cyber Security and Information Assurance (OCSIA) and Research Councils UK (RCUK). The Centres 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.

Those currently recognised are: Imperial College; Lancaster University; Newcastle University; Queens University Belfast; Royal Holloway; University College London; University of Birmingham; University of Bristol; University of Cambridge; University of Oxford; University of Southampton.

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 status, 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.

Where can I find more details?

Further details on the scheme can be found on the CESG website http://www.cesg.gov.uk/awarenesstraining/academia/Pages/Academic-Centres.aspx or by emailing academia@gchq.gsi.gov.uk

Research Institutes in Cyber Security

The opportunity to engage

Research Institutes are virtual entities facilitating collaboration between leading researchers. The first EPSRC-GCHQ Research Institute, in the ‘Science of Cyber Security’ is a virtual organisation involving seven universities, Directed by Professor Angela Sasse of University College London. Its £3.7m programme brings together leading academics in the field of cyber security – including social scientists, mathematicians and computer scientists – from across the UK. Their work will help to answer two common questions faced by organisations: how secure are we, and how do we make better security decisions?

The second EPSRC-GCHQ Research Institute is in Automated Programme Analysis and Verification, led by Professor Philippa Gardner of Imperial College London. Its partners across six leading UK universities will investigate new ways of automatically analysing computer software to reduce vulnerability to cyber threats. Its creation recognises the excellence of UK research in this key aspect of cyber security.

A third EPSRC-CPNI Research Institute has been announced in Trustworthy Industrial Control Systems.

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 RIs will help ensure better articulation with business problems and opportunities around cyber security.

Where can I find more details?

Further details on the RIs may be obtained by emailing: academia@gchq.gsi.gov.uk

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** will deliver multidisciplinary training that provides the skills needed by the UK's next generation of doctoral-level cyber security experts. In doing this, centres will engage with businesses to ensure that this training reflects the complex and dynamic nature of cyber threats. Training will last for 4 years and comprise a formal assessable programme of taught courses (equivalent to Masters-level) in a range of subjects addressing key areas of cyber security and a related challenging and original research project. Both centres will between them produce at least 66 graduates and graduates will have the ability to contribute research-derived expertise to business or HMG.

The **Oxford University CDT** will focus 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.

The **Royal Holloway CDT** will focus on problems faced by businesses and government such as: provably-secure cipher systems and protocols, systems engineering and security analysis, trusted and trustworthy platforms and organisational processes and socio-technical systems

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.

Where can I find more details?

For further details, please contact

University of Oxford

Mrs Maureen York,

CDT in Cyber Security,
Department of Computer Science,
Wolfson Building, Parks Road,
Oxford. OX1 3QD
Phone: (+44) (0) 1865 283569

Email: cdt@cybersecurity.ox.ac.uk

Royal Holloway, University of London

Dr Carlos Cid, Director
CDT in Cyber Security
Royal Holloway, University of London
Phone: +44 (0)1784 414685
email: cybersecuritycdt@rhul.ac.uk

Initiatives supporting new or existing cyber security professionals

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 is coming together through e-skills UK 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 a common language that professionals, public and private sector employers, and training providers can all use to benchmark information security skills.

Providing the building blocks of qualifications and training programmes, the standards help industry identify skills gaps, and define new learning and career pathways to fill them.

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.

Benefits to employers

Employer involvement in new pathways development will improve the prospects for their design maximising utility and relevance for their particular business 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.

Where can I find more details?

Contact Nigel Payne at e-skills UK at nigel.payne@e-skills.com.

CESG Certified Professional (CCP) Scheme

Opportunity to engage

GCHQ has established a new 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.

CCP assess candidates at three levels of competence over 6 roles (soon to be 7 with the introduction of the Penetration Tester one). The skills required to perform each role are based on skills and skill levels developed by the Institute of Information Security Professionals (IISP) www.iisp.org/ The roles currently certified are: Accreditor, S&IRA, Architect, Auditor, IT Security Officer, Comms Security Officer.

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 for GCHQ by three certification bodies: APM Group, BCS and IISP (with Crest and RHUL). All scheme 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 employees and suppliers are CESG Certified Professionals.

Benefits to employers

Employers supporting and promoting use of the scheme and its further development, can help ensure 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.

Where can I find more details?

By emailing: profcert@CESG.GSI.GOV.UK or by visiting http://www.cesg.gov.uk/awarenesstraining/IA-Certification/Pages/index.aspx

Certified Training Scheme

Opportunity to engage

GCHQ has established a new certification scheme for cyber security professionals known as Certified Training.

Training providers will have the opportunity to submit their cyber security courses to a CESG-approved Certifying Body (CB). The courses will be assessed by the CB against a CESG- approved standard which will measure both course content and delivery. This provides a level of confidence to course attendees that the subject material and the teaching are at an approved level. The basis for the scheme is to provide training in support of the CESG Certified Professional(CCP) roles, so whilst it might apply to someone new to Cyber Security, or someone seeking to enhance their skills, it will suit an individual who aspires to gain or enhance professional status through CCP. The syllabus will be based on the core skills in the Standard document, many of which will be common to most of the portfolio roles.

A small number of courses will have been assessed by the end of Summer 2014.

Organisations can get involved by:

- once the scheme is launched, 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 Certifying Body for CESG certification;
- providing regular feedback on the quality of content and delivery of Certified Training courses to the Certifying Bodies.

Benefits to employers

Participating employers can have confidence that specific courses certified under the scheme provide a good standard of training in terms of cyber security content and delivery. The syllabus will be based on the core skills required for CCP roles and provide the basis for a learning pathway into HMG’s professional standard for cyber security.

Where can I find more details?

Further details on the Certified Training scheme may be obtained by emailing:

profcert@CESG.GSI.GOV.UK

CompTIA support ex-military professionals into IT jobs through ‘Armed for IT Careers’

The opportunity to engage

CompTIA, the global IT trade association, is helping solve both the IT skills gap and the growing number of ex-service professionals struggling to find jobs by launching Armed for IT Careers.

Armed for IT Careers provides a one-stop-shop for transitioning and ex-military personnel to learn about a career in IT, find training, find resettlement funding, get qualified and land their first IT job.

The programme provides service-leavers with education, credentials and job placement resources to be successful in this exciting sector and allows employers to show their support. Veterans with the right mix of business, communication and technical skills can find long-lasting and rewarding careers across the IT industry and be a great asset to an organisation.

Employers can

- Show support for the initiative by joining a registry
- Commit to recruit ex-service personnel
- Provide logo and links to career/landing page with open positions
- Provide news or success stories

Benefits to employers

Employers offering such support can get direct access to skilled and highly motivated individuals that are keen to learn new skills, security cleared and eager to look for their next challenge following service.

Where can I find more details?

Learn more at www.armedforitcareers.org

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.

Where can I find more details?

Please contact queries@cybersecuritychallenge.org.uk

CREST supports learning pathways and career development

CREST supports industry and career development through its Academic Partnership Programme, professional development, training and conferences. Key to this is a commitment to information sharing, encouraging closer relationships between the academic community and industry and creating a profession with well-defined career paths. Extensive research on a variety of information assurance topics is carried out and made available to industry and Government alike.

There is an acute shortage of skilled individuals in the technical information assurance community. This drives the need to encourage the very best into this sector to support demand in the industry and the growth of member companies. But to attract the brightest young people and encourage good people to change career, we must create a profession with clearly laid out career paths.

Training Partners - CREST recognises the need for professional development programmes and works closely with e-skills UK to develop occupational standards. CREST also works with others to develop learning pathways into the sector and assists training course providers with a defined structure to develop courses.

Academic Partners - CREST is also 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 your studies.

Benefits to employers

If the technical security industry is to be viewed as a profession and attract the best, it must demonstrate worthwhile industry-recognised professional qualifications, with an enforceable code of conduct. CREST provides both: its qualifications are the gold standard for technical information security and if member companies don’t 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. While CREST is helping students to discover the opportunities in this sector by studying at leading universities offering information assurance courses.

We are at a pivotal point. If we work together we can create a real profession where business can flourish and the very best people can have a great career. CREST want to make the information technology world a safer place – get involved and help us realise a global goal.

Where can I find more details?

Further details on the activities of CREST can be found at www.crest-approved.org

CREST

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

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

BIS/14/649