WHITE PAPER

# PERSPECTIVES:

## Integrating Cybersecurity into Computer Science Curricula

## SUMMARY

Cybersecurity is one of the fastest developing and evolving requirements within industry and government today as online, connected and mobile systems make up the foundations of a digitally-enabled economy.

Universities help provide, support and develop talent through undergraduate, graduate and professional development programmes. At the undergraduate level most institutions offer three year Computer Science degree courses in which there is some element of security provision, though this may not constitute a large mandatory part of courses. Furthermore, explicit reference to the need to develop skills in cybersecurity are often absent even if the content covers the topic adequately.

It has been suggested that this leaves a gap between a developing industry requirement and the skills computing science graduates are equipped with throughout their course of study. The implications go beyond the challenges new graduates may face as they enter the workforce: It touches on the ability of all organisations and government to deliver goods and services in a highly connected, technology-dependent and highly besieged digital landscape. It is increasingly contended that computing science without security perpetuates the development, design and maintenance of computing systems that won't be fit for purpose for this business environment.

> ***"It is increasingly contended that computing science without security perpetuates the development, design and maintenance of computing systems that won't be fit for purpose for this business environment."***

This paper explores the evolving role of cybersecurity covering areas such as information security, systems security, application security and information assurance – the impact being felt across society of poor attention to cybersecurity, as well as the prospects for addressing growing expectations from industry and government, including those laid out in the new Key Information Set (KIS)[1] which are being mandated by the Higher Education funding councils for all Higher Education Institutions (HEIs).

We suggest that exposure to more cyber and information security concepts at the undergraduate level could have a variety of benefits for the students, the academic institutions, industry and society. However, it must be recognised that to have any profound impact the effort must be collaborative between industry, professional bodies and academia.

## SITUATION ANALYSIS

Industry and Government alike are grappling with the ever increasing challenge of securing systems and information, as the rate of emerging cyber threats continues to grow in the expanding digitally–enabled economy. The need for talent in cybersecurity has become a national priority with studies showing double digit growth rates in the projected workforce for cybersecurity. The most recent (ISC)$^2$ Global Information Security Workforce Study, commissioned by the International Information Systems Security Certification Consortium (ISC)$^2$ and conducted by industry analysts Stratecast (a division of Frost & Sullivan) projects the workforce in cybersecurity to double within five years, with 11 percent year on year growth.[2] Hostile attacks on UK cyber space were classed as a tier 1 national threat within the 2010 National Cyber Security Strategy for the United Kingdom, alongside terrorism, natural hazards or flu pandemics and the threat of military conflict.[3] This is a consequence of the potentially enormous impact a successful attack could have on the IT systems supporting the UK government, UK critical national infrastructure, business and the economy.

Universities are being called upon to provide, support and develop this much needed talent with opportunities to incorporate cybersecurity content across a broad curriculum set for undergraduate, graduate and professional development programmes. Twenty years ago very few courses paid any significant attention to security, and the situation has started to change, albeit

[1] The KIS is a report which includes information from the National Student Survey (NSS) and the Destination of Leavers from Higher Education (DLHE) ee: www.hesa.ac.uk
[2] https://www.isc2cares.org/IndustryResearch/GISWS/
[3] www.cabinetoffice.gov.uk/reports/national_security_strategy.aspx

slowly. Currently most institutions offer courses in which there is one module or unit – approximately 5 percent of the total credits in a degree - dedicated to cybersecurity in a core three- year Computer Science degree.

In contrast, there is a growing voice from industry that cybersecurity knowledge should be core to the disciplines of computing and information technology (IT) and therefore a key element of the computing and computer science curriculum, particularly at the undergraduate level. It is recognised that security is a requirement for all systems, yet not all systems are developed with security as a requirement. By instilling the relevant security knowledge during their education, computing professionals will have a better appreciation for the need to develop and maintain systems able to withstand cyber threats.

Computer Science graduates should be in a strong position to consider the growing number of careers and roles that are focussed on cybersecurity and related disciplines. These range from specialist areas such as cyber forensics to consultancy and the broad career path that leads to senior management as Chief Information Security, Chief Risk or Chief Security Officer. Currently employers report that they are looking to a wide-ranging set of graduates to fill these roles, and that computing science graduates are not necessarily their first port of call, despite the understanding of technology that is required in the majority of these areas.

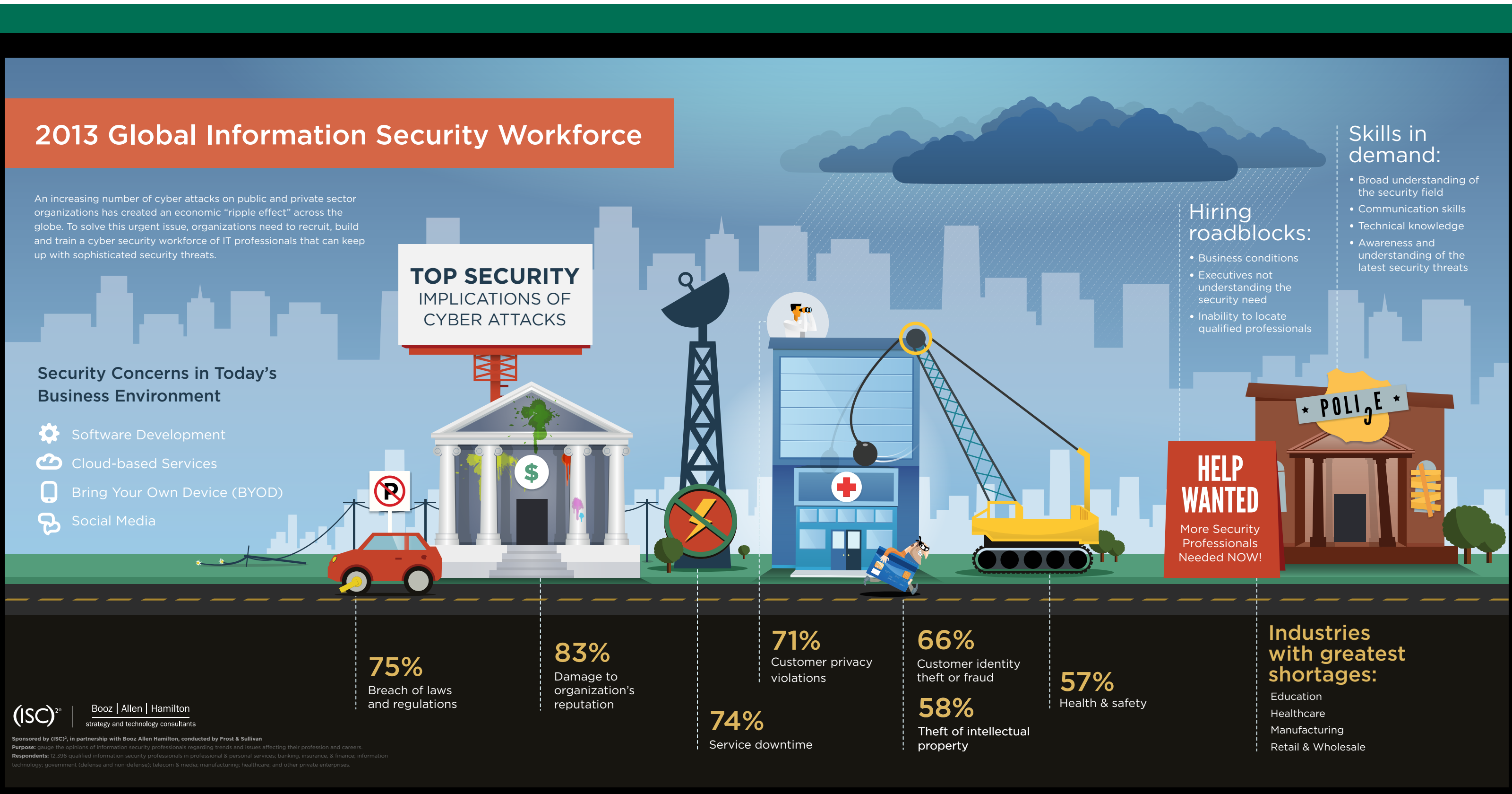
The Key Information Set (KIS) for university courses, established in 2012 as an indicator of the quality and effectiveness of degree courses, puts a significant emphasis on the employability of graduates. The data included in the KIS of a course includes data on the destinations of students after graduation. Overall, Computing Science graduates (there is no breakdown available for digital security specifically) are reported to have experienced high levels of unemployment since the system was put in place with 2012 data indicating that 17 percent were not in full time work six months after graduation;[4] and 2013 data showing an improvement with 13 percent not in full time work after graduation. In both years, this level is higher than graduates from other subjects. While the reported reasons for this are varied, the figure sits in sharp contrast to the reported demand for talent in cybersecurity.

In addition to the prospects for employment, the opportunities are also rich for graduates interested in moving on to post-graduate study, another area tracked within the KIS, with many established masters' level programmes in cybersecurity. An initiative from the Government Communications Head Quarters (GCHQ), the UK government's intelligence and security organisation, to accredit Masters degree programmes has been launched, while the GCHQ also oversee a government- led scheme to recognise Academic Centres of Excellence for Cybersecurity Research.[5]

Given the size of the requirement, accreditation for computing science degrees is now being updated to include mandatory learning outcomes for cybersecurity by 2016 for all university courses that are to be accredited by the Institution of Engineering & Technology and the British Computer Society (BCS ,The Chartered Institute for IT). With up to 25 years of documented experience pioneering professional bodies, sectors skills councils and industry groups, as part of their strategic plans to address the skills gap, are now working to make their knowledge readily available to support course development, and to work with educators in the effort to support its delivery.

[4] Destinations of Leavers from Higher Education (DHLE) Survey, 2011-12, HESA, http://www.hesa.ac.uk

[5] https://www.gov.uk/government/publications/cyber-security-research-capability-academic-centres-of-excellence



## 2013 Global Information Security Workforce

An increasing number of cyber attacks on public and private sector organizations has created an economic "ripple effect" across the globe. To solve this urgent issue, organizations need to recruit, build and train a cyber security workforce of IT professionals that can keep up with sophisticated security threats.

**TOP SECURITY**
IMPLICATIONS OF CYBER ATTACKS

**Security Concerns in Today's Business Environment**

- Software Development
- Cloud-based Services
- Bring Your Own Device (BYOD)
- Social Media

Hiring roadblocks:

- Business conditions
- Executives not understanding the security need
- Inability to locate qualified professionals

Skills in demand:

- Broad understanding of the security field
- Communication skills
- Technical knowledge
- Awareness and understanding of the latest security threats

75% Breach of laws and regulations

83% Damage to organization's reputation

74% Service downtime

71% Customer privacy violations

66% Customer identity theft or fraud

58% Theft of intellectual property

57% Health & safety

Industries with greatest shortages:

- Education
- Healthcare
- Manufacturing
- Retail & Wholesale

(ISC)²® | Booz | Allen | Hamilton
strategy and technology consultants

**Sponsored by (ISC)², in partnership with Booz Allen Hamilton, conducted by Frost & Sullivan**
**Purpose:** gauge the opinions of information security professionals regarding trends and issues affecting their profession and careers.
**Respondents:** 12,396 qualified information security professionals in professional & personal services; banking, insurance, & finance; information technology; government (defense and non-defense); telecom & media; manufacturing; healthcare; and other private enterprises.

# INDUSTRY PERSPECTIVE

Organisations of all sizes, from the small and medium business to the multinational, are facing phenomenal change, driven by the opportunities and benefits afforded by being connected and online. Developments continue apace across what is known in security circles as the "the threat landscape", with activists, terrorists and the wider criminal community recognising the opportunities to move their activities online. As a result, cybersecurity has moved up the priority list, particularly with regards to the protection of sensitive data.

Clearly this environment requires companies to take ever more significant steps to protect their own and their customers' information, no matter what format that information takes. The first step in this process is to understand the fundamental implications this has for systems and product design, and management. By and large this first step has yet to be taken and so companies are currently wrapping security measures around systems that regularly contain vulnerabilities and faults, often allowing them and therefore the business they support, to be easily compromised. A cursory consultation of the UK Information Commissioner's Office (ICO) web site demonstrates the impact this situation is having, with organisations seeing their reputation undermined and facing fines of up to half a million pounds for a single breach of sensitive data.

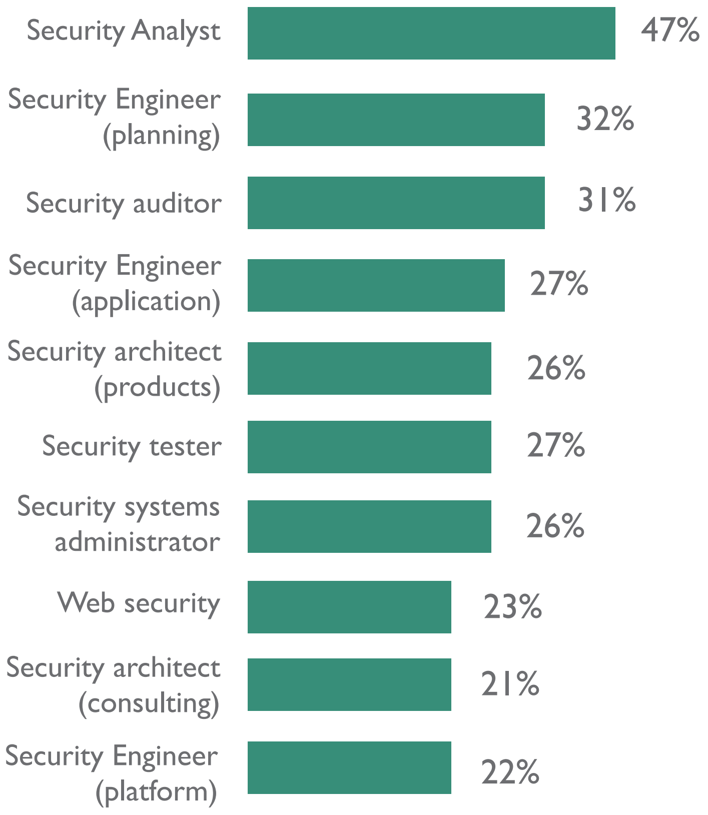
> ***"We can no longer afford to tolerate relatively simple security problems like those presented in this OWASP Top 10."***

Particularly concerning is the simplicity, frequency and repetitive nature of some of these faults, which can be found in both commercial and consumer products and software. For example the Open Web Application Security Project (OWASP)[6], a voluntary effort dedicated to enabling organisations to develop trusted applications, regularly publishes a list of software faults which has not changed significantly in the past 10 years.[7] As they published their most recent list in 2013 they lamented the poor attention it seemed to be getting from the software development community as a whole, saying: "Insecure software is undermining our financial, healthcare, defense, energy, and other critical infrastructure. As our digital infrastructure gets increasingly complex and interconnected, the difficulty of achieving application security increases exponentially. We can no longer afford to tolerate relatively simple security problems like those presented in this OWASP Top 10."

Topping the list for frequency and persistence is the SQL injection attack whereby external, untrusted data can be sent to execute a command or query, tricking the interpreting system into providing access to the company's system or data and bypassing proper authorisation. There are at least three well-documented fixes available for this concern, yet its prevalence continues. Another Top 10 concern is the use of components with known vulnerabilities including framework libraries which can easily be exploited with the use of automated tools.

Organisations require people with the skills and perspective to work in this business environment, but they are said to be struggling to find them. For cybersecurity in particular an emerging gap in the availability of people with required skills is beginning to have an impact. Looking beyond growth projections, the 2013 (ISC)$^2$ Global Information Security Workforce Study reveals that open information security positions are remaining unfilled contributing to declining levels of confidence in companies' ability to defend against breaches. It also cites the rapid introduction of new technologies that don't have security "baked in" the product development process as a contributing factor to stresses being reported by short-staffed security teams, emphasising that this is happening at a time when organised attacks are on the increase.

## Shortages by Job Titles (Top 10)



[6] See: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
[7] https://www.owasp.org/index.php/Top_10_2013

Overall, 56 percent of those participating in the study felt their organisations had too few people with the necessary cyber skills to manage the current workload and nearly half of the respondents admitted that this shortage is having an impact on their customers. When asked to rate the most important success factors for an information security professional, "a broad understanding of the security field" was identified. Delving deeper, the skill set most in demand reflected a wide remit: the security analyst who conducts the integration and testing, operation, and maintenance of systems security. This security analyst is also required to have a deep understanding of all business systems, and an appreciation for what information an organisation cannot afford to lose.[8]

There is a need to improve cybersecurity knowledge and appreciation across perspectives from technology use to the business decision making, procurement and the Information technology (IT) function itself. In the very largest companies, a dedicated security department is likely to drive a strategy to meet this need, but it has high cross-department dependencies, relying on the development of cyber competencies within the IT department and business units as well. The vast majority of smaller organisations will rely on external professional services, their IT team or both to drive this strategy.

## THE GOVERNMENT PERSPECTIVE

The Government's objective is to better protect the nation's interests from a defence, economic opportunity, efficiency and societal public safety point of view. With cyber threats classed as a tier 1 threat, there is an admission of concern around the potential impact of the growing variety and sophistication of threats.

The threat however, is only one perspective driving the Government's Cybersecurity Strategy. Dependencies and opportunities generated by good cybersecurity for economic growth are regularly touted by various government officials. Ambitions set out by UK Trade and Investment, The Cabinet Office, The Department for Business Innovation and Skills and others are to take advantage of the UK's current European-leading position in the field and establish it as an economic hub, akin to that of the UK financial services sector today. On the release of a cross-department report[9] on the national cybersecurity skills strategy in March 2014, then Universities and Science Minister David Willetts said: "Today countries that can manage cybersecurity risks have a clear competitive advantage. By ensuring cybersecurity is integral to education at all ages, we will help equip the UK with the professional and technical skills we need for long-term economic growth." The overarching national cybersecurity strategy is written around four strategic objectives:

- Making the UK one of the most secure places in the world to do business in cyberspace
- Making the UK more resilient to cyber attack and better able to protect our interests in cyberspace
- Helping shape an open, vibrant and stable cyberspace that supports open societies
- Building the UK's cybersecurity knowledge, skills and capability.

> ***"Ambitions are to take advantage of the UK's current European-leading position in the field and establish it as an economic hub, akin to that of the UK financial services sector today."***

In response, government activity and policy reflects the need to motivate the widespread development of new capabilities both within government and UK industry generally. There is an emerging regulatory agenda aimed at drawing attention to and sanctioning ignorance of very addressable oversights, such as those outlined in the OWASP TOP 10 and ICO. Policy and funding initiatives are being developed to motivate a societal response to the need, with particular attention being made to enhancing the academic and education community's ability to help industry and society flourish in this digitally-enabled world. For example, the UK's Department for Business and Innovation Skills (BIS) this year outlined plans for skills and funding packages aimed at developing initiatives for graduate and post graduate students, as well as internships and apprenticeships.[10]

> ***"By ensuring cybersecurity is integral to education at all ages, we will help equip the UK with the professional and technical skills we need for long-term economic growth."***
>
> **- David Willets,** Minister for Universities and Science 2010-2014

Through 2014-15 the National Cybersecurity Skills Plan (NCSP) includes activities to strengthen the supply of cybersecurity skills as part of a wider strategy to enhance all digital skills across the economy. Activities to date have included collaborating with universities to embed cybersecurity into a range of software engineering and computing degrees, including:

8. (ISC)$^2$ report Critical Times Demand Critical Skills: An analysis of the skills gap in information security, (ISC)$^2$ 2014, https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/GISWS-Skills-Gap-Analysis.pdf
9. Cybersecurity Skills, Business Perspectives and Government's Next Steps supporting evidence , March 2014
10. Cybersecurity Skills, Business Perspectives and Government's Next Steps, March 2014

- Funding for the National Centre for Universities and Business (NCUB) which develops, promotes and supports collaboration between universities and businesses across the UK[11]
- Higher Learning Apprenticeships programmes that have been developed with eSkills UK[12], the industry supported sector skills council for business and information technology
- The Trusted Software Initiative, which has developed a specification for good practice in secure software development: PAS 754 'Software trustworthiness – Governance and management – Specification[13]
- A range of initiatives under the National Cybersecurity Programme (NCSP) and GCHQ including granting Academic Centres of Excellence in Cybersecurity Research status to universities, accreditation for Masters Level Programmes and funded centres for Doctoral Training to develop high-end skills and capabilities.

Increasing attention is turning to the need to provide specialist education to address the gap in academic provision of cyber education at the undergraduate level. Currently, there is significant development in postgraduate programmes for cyber and information security – with over 55 such courses across the UK. A review of graduate course registrations suggests however that UK undergraduates are not taking up places on Masters'-level courses in cybersecurity: The majority of places are taken up by students already in employment and international candidates, with many courses designed to accommodate the study around full-time work. Exposure to more cyber and information security concepts at the undergraduate level could equip more of the future workforce with the cyber skills required in the digitally-enabled economy whilst also offering a clear opportunity for students to discover and consider a pathway for a new generation of IT or specialist security professionals.

## SOCIETY'S PERSPECTIVE

The digitally-enabled economy yields benefits across all strata of society including, but not limited to:

- Ecommerce leads to more efficient, more convenient ways of doing business
- Smart cities/smart grids leads to enhanced energy efficiency
- Connected healthcare enhances patient experience and outcomes by more efficient and immediate access to relevant medical data
- Online banking and shopping allows people more time for other priorities
- Online learning makes education more accessible to many
- Social networking enables more people to be connected to friends, family, job opportunities and more.

In short the convenience, efficiency and new capabilities afforded by working and connecting online has ensured that everyone is functioning within the digitally-enabled economy at some level. Many companies, services and even tax and local council services can only be accessed online. Particularly with younger generations, much of their lives are documented and easy to find online. As people interact with companies and public services and freely offer personal information, they do so with an implicit belief that the associated risks in doing so will have been considered and managed. However the gap in understanding and mitigating these risks within the development of the systems that they are interacting with suggests that this trust is often misplaced.

Fortunately, as more breaches of sensitive data make news headlines, public appreciation for the risks is now developing. People are increasingly recognising that they are dependent on the digitally-enabled economy and that a by-product of this is the availability of massive amounts of their personal data in connected and online systems. Phenomenal rates of identity theft, fraud, damage to reputation, bullying and other risks are shaping public awareness, and in turn leading online companies to seek to reassure by actively communicating their commitments to cybersecurity.

Further, poor cybersecurity, or the perception that information will not be protected or may be sold on to other organisations, is now beginning to seed public backlash against the use of digital platforms. This was quite clearly illustrated by the recent unease over the NHS care.data project[14], which was has experienced significant delay in response to public concern over poor communication over the security measures that had been put in place to secure the medical data that all UK citizens were being asked to release into the project, and how the data could be used and passed on to other organisations.

Landmark court judgements are also demonstrating the strength of expectation mounting within society for more control over the data that is collected, manipulated and distributed by companies and their IT systems, whether it was freely given or not. The May 2014 ruling from the European Court of Justice granting a Spanish man the right to have links to a 1996 local newspaper story about his bankruptcy removed from Google's search engines, effectively grants a "Right to Erasure" that the EU government has

[11] Cybersecurity Skills, Business Perspectives and Government's Next Steps – supporting evidence , March 2014

[12] https://www.e-skills.com/

[13] PAS 754 'Software trustworthiness – Governance and management – Specification , June 2014 http://www.uk-tsi.org.uk/

[14] See, for example: http://www.england.nhs.uk/ourwork/tsd/care-data/, http://www.computerweekly.com/blogs/editors-blog/2014/02/the-lesson-from-the-nhs-careda.html

been advocating in its proposed Cybersecurity Strategy for 2016. Public judgement against eBay too showcased an expectation that personal data, not just financial transactions should be encrypted. As the digitally-enabled economy develops, cybersecurity is increasingly seen by society, as well as governments, to be at the heart of its healthy development. Dependency on vulnerable systems is recognised to present a personal risk to individuals and their lifestyles, not just the businesses and services with which they interact.

## ACADEMIC PERSPECTIVE

Supporting the development of the workforce is not a trivial exercise. While there are many calls for academia to be demand-led in its development of new programmes, there must always be an element of supply-led development as most technological enhancements that have shaped society and business have origins in academic research. There are also calls for ensuring the supply of "oven-ready" graduates. However, by purely considering Computing courses as vocational (and it should be noted that there exist a number of very good theoretical computer science courses) fails to recognise the important transferable skills that are developed in these courses. Hence striking the correct balance in programme development is a key consideration, and something academics continually strive to achieve.

The Destinations of Leavers from Higher Education (DLHE)[15] survey, overseen by the Higher Education Statistics Agency (HESA) each year (and included in the KIS), shows that Computer Science degrees reflected the highest level of unemployment of the 19 subject areas reviewed, with 17 percent of graduates unemployed six months after graduation in 2012; and 13 percent after graduation in 2013.

> *"the UK government is encouraging greater collaboration between industry, the practicing profession and the education providers that supply it with new talent."*

Computer Science employment rates were actually comparable with other subjects, but far fewer graduates from the discipline undertake postgraduate study. Acknowledging this outcome as an area of concern, the Council of Professors and Heads of Computing (CPHC) commissioned a subsequent report which gave an unemployment figure for Computer Science graduates at 14.7 percent compared to 9.1 percent for all graduates[16]. The breadth of the CPHC report suggested that the reasons for the comparatively high figure are varied. The report highlights the opportunity to address the concern of bridging the disparity between graduate skills and industry requirement, as highlighted by the key information set for employability. The challenge remains however that industry expectations are not clearly defined, while the subject matter that comes under the computer science umbrella continues to grow.

Among suggestions for improvements were to augment courses with content that address the growing requirement for skills that are in demand in the UK IT market. Given the demands that are developing for cybersecurity skills, this is an area that presents a good opportunity for course designers as they set out to make these improvements.

Currently, when companies are recruiting for specific roles related to cybersecurity, computing science graduates do not necessarily have an advantage over graduates of other disciplines, despite the need for technical as well as security knowledge within these roles. This revelation was given by hiring managers participating in a workshop Developing Cybersecurity Talent for the UK in 2013[17], hosted by (ISC)$^2$ and the Council of Professors and Heads of Computing to bring together invited participants from academia and industry. The contention was that it was better to teach a business or management graduate what they needed to know about technology than the reverse. The current consensus is that supervisory cost of placements is very high for companies to take on many graduates of any kind in cybersecurity roles.

While work is currently underway to embed secruity requirements within accreditation criteria, for courses to date, accreditation from BCS and IET, which between them accredit the majority of computing, computer software, computer science and engineering degrees in the UK, could be achieved by addressing security at a high, somewhat superficial level. No reference to specific knowledge or effort to embed such knowledge within a particular subject domain has thus far been needed.

Some employers and prospective students will consider courses through information that is available through UCAS, the Universities and Colleges Admissions Service. However, there does not appear to be clear and explicit reference to security within many courses listed here. This would suggest that for some courses at least security content is covered within an optional module. Many of the lecturers participating in the earlier mentioned workshop confirmed that anything beyond basic security principles were covered as an optional subject. They also stated that these modules

[15] Destinations of Leavers from Higher Education (DHLE) Survey, 2011-12, Higher Education Statistics Agency (HESA)

[16] CS Graduate Unemployment Report 2012, Council for Professors and Heads of Computing, http://cphcuk.files.wordpress.com/2013/12/cs_graduate_unemployment_report.pdf

[17] Developing Cybersecurity Talent for the UK, Bedfordshire, 2013, a joint workshop from CPHC and (ISC)$^2$ )bringing academia and industry together to discuss challenges in attracting and educating raw talent

are not often selected by students, suggesting that they may not be valued and thereby leaving security to be a disparate and poorly addressed subject within their programmes. Industry participants on the day felt that such an approach denies the context required to ensure an understanding of the impact cyber and information security has on systems, and perpetuates the belief that cyber and information security is a narrow specialist subject. This notion is in sharp contrast to the breadth of skills and understanding of security concepts that is being sought after by industry.

The growing consensus from industry and government is that people with responsibilities in Information or Communications Technology , not just those with focussed security roles, must have an understanding of cybersecurity in order to meet the needs of a digitally-enabled economy, and to prevent the continued proliferation of security vulnerabilities and flaws at the systems design stage. Academia has not completely ignored the subject: Security was identified as one of the top three concerns at the CPHC annual conference for 2014.The challenge ahead is to define and understand the breadth of the requirement and appreciate the basics or principles of cybersecurity that relate to the context of the particular course of study.

Such an effort can be a catalyst for good prospects for graduates seeking employment in the current IT environment, exposure to an area for specialisation later in their career, or the pursuit of further study with a healthy choice of postgraduate courses relating to cybersecurity.

## Standardising Skill and Competency Expectations

Despite the relative immaturity in the field, there is a wealth of documented knowledge of cybersecurity practice. Organisations, industry groups and grass roots efforts to establish professionalism have succeeded in federating tried, tested and accepted practices and professional certification programs that employers have come to rely upon in recruitment for and strategic management of the cybersecurity needs. Most have or are developing programmes for universities representing a rich and willing resource for academics and course designers seeking to embed cybersecurity within their programmes. For example:

- The (ISC)$^2$ Global Academic Program provides accredited academic institutions access to resources and support based on the (ISC)$^2$ common body of knowledge (CBK®)

### Table 1: Example Approaches and Collaborations

| Requirements | Established Approach | Collaboration |
|---|---|---|
| Develop university accredited degree courses | • Certification organisation can work alongside accrediting professional bodies<br>• Professional bodies include content from information security qualifications as part of undergraduate programme<br>• Universities encouraged to provide degree courses which include a strong link to a professional qualification | Academia, Government & Professional Bodies (IET, BCS, (ISC)$^2$, etc. |
| Equip more CS graduates going into industry with the requisite cyber and information security skills | • Employers define course content in line with skills and abilities they need in their businesses. Graduating students have a greater chance of meeting these needs and gaining employment<br>• Students engage with employers throughout the duration of their course. They develop the critical skills they need and employers gain early access to students and recruit the graduates who fit their business<br>• Universities have access to employer involvement in both course creation and delivery, so programmes remain current and fit for purpose | Academia & Industry brokered by professional community/bodies |
| Raise profile of cybersecurity as new discipline with good career possibilities | • Utilise government and industry funded initiatives such as the Cybersecurity Challenge<br>• Enrol in programs similar to Cybersecurity Skills Alliance to provide further academic progression for graduates | Academia, Government & Industry |

covering its members practice disciplines within information security, software security, forensics, and healthcare[18];

- CREST Academic partners Programme for Assurance in Information Security with resources covering penetration testing and incidence response[19].
- Institute of Information Security Professionals (IISP) which manage the frameworks that form the basis for the UK CESG Certified Professional Scheme[20]
- ISACA, which has education materials based on the COBIT Framework for professors and teachers[21]

Such efforts are driven by a recognition that universities provide a valuable and much-needed filter, development platform and support structure for raw talent. There is also acknowledgement that the skills gap is so significant that the strength of university system is needed to bring in the number of employees required. While it can be argued that many courses could benefit from enhancing the cyber content, computing science courses are a primary target.

As already noted, the UK government is encouraging greater collaboration between industry, the practicing profession and the education providers that supply it with new talent. This includes funding through the Higher Education Authority for innovative proposals for curriculum development that reflects this. In support of this, the Government's Office of Cybersecurity and Information Assurance (OCSIA) is working alongside the IET and the BCS as they update their accreditation guidelines to address the need for cybersecurity. From 2016 all university courses that are to be accredited by the IET and the BCS are to deliver mandatory learning outcomes around cybersecurity.

Cyber skills requirements, identified by stakeholders and addressed using established approaches, can provide a guide to understanding how existing Computer Science degree programmes across UK universities can be augmented to meet these developing expectations. While much development in this area remains in the formative stages, we can identify approaches that are becoming established. Table 1 (page 7) provides a high-level view of effort being undertaken by the programmes referenced in this paper, including e-Skills UK, The Trusted Software Initiative (TSI), (ISC)$^2$; and CREST/IISP.

Where examples of stakeholder collaboration have been undertaken, the outcomes have been positive. e-Skills UK reports on its Software Development for Business degree that "universities currently involved with e-skills degrees have seen an increase in student numbers, an improvement in the gender balance on the course and a significant increase in employability rates"[22].

Such a collaborative approach in the development of university undergraduate computer science courses, which address the shortfall in information security education, can be expected to deliver gains to Key Performance Indicators (KPI) for all stakeholders, aligned to their main objectives (see Table 2).

## Table 2: Stakeholder Objectives and KPIs

| Stakeholders | Academia | Industry | Government |
|---|---|---|---|
| Objectives | Improvement to the KIS | Recruitment of skilled staff | Dept. for BIS, Objective 423[23] |
| KPI | • Better qualified graduates<br>• lower CS graduate unemployment<br>• Accredited degree courses | • Broader understanding of the security field<br>• Better technical skills<br>• Awareness and understanding of the latest security threats | • Stimulated HE student interest and raised profile of cybersecurity as new discipline with good career possibilities<br>• Development of a community of cybersecurity research being carried out in the UK<br>• The UK more resilient to cyber-attacks and crime |

[18] https://www.isc2.org/global-academic-program/default.aspx

[19] http://www.crest-approved.org/training-and-academia/academic-partners/

[20] https://www.iisp.org/imis15/iispv2/Accreditation/CCP_Info.aspx

[21] http://www.isaca.org/Knowledge-Center/Academia/Pages/Educational-Materials-for-Professors-and-Teachers.aspx

[22] e-Skills UK, 2014 http://www.e-skills.com/education/e-skills-degrees/e-skills-software-development-for-business-degree/

[23] The department for BIS objective 4 is: Building the UK's cybersecurity knowledge, skills and capability, Progress against the Objectives of the National Cybersecurity Strategy – December 2013

## Conclusions

Government and industry alike are looking to universities to assist in addressing the need for new talent across a great many disciplines in the digitally-enabled economy. Cybersecurity is a discipline that is receiving great attention, funding and recognition as a specialist area experiencing double digit growth in the workforce. There is a clear opportunity and impending mandate for computing science courses to help their students take advantage of this and improve course outcomes as measured by the Key Information Set. Currently computing science graduates do not appear to have a clear advantage when it comes to cybersecurity roles, nor do they reflect the breadth of knowledge in security that also is needed within the connected information technology workplace.

While the task ahead is significant, universities are not required or able to tackle the issue in isolation; approaches are becoming established to underpin collaboration with industry and professional bodies, where the knowledge and understanding of competency requirements currently resides. With such a collaborative approach academia can join the UK industry and government in the effort to ensure society and our economy can be better equipped to thrive in the digital age.

## About (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 nearly 100,000 members in more than 135 countries. Globally recognized 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**.

## About CPHC

The Council of Professors and Heads of Computing (CPHC) is open to Professors and/or Heads of Computing Departments (or related subject groups) in all UK Universities within the United Kingdom (UK). With nearly 800 individual members, drawn from relevant schools and departments in over 100 UK universities, the CPHC has the mandate to be the representational body for this group in the UK and as such the CPHC is consulted by policy-makers and practitioners undertaking any activities that affect the sector. For more information **cphc.ac.uk.**

## Authors

**Professor Carsten Maple**
Vice Chair, Council of Professors and Heads of Computing
Professor of Cyber Systems Engineering
Director for Cyber Security Research
WMG, University of Warwick

**Adrian Davis**, PHD, MBA, FBCS, CITP
Managing Director
(ISC)² Europe Middle East & Africa

**Iain Millar**, PhD, CISSP, MIET
eSkills and Careers Group Lead
EMEA Advisory Board
(ISC)² Europe Middle East & Africa