Cybersecurity to Become Core Component of UK Computing Degrees

Consortium of industry, academia and government bodies create cybersecurity learning guidelines to be embedded into BCS accredited UK Computer Science and IT-related degrees

- New embedded course guidelines and learning outcomes support Government Cyber Security Strategy.
- Resource for universities designed to solve critical cyber threats to UK economy by embedding cybersecurity into the core of computing degrees.
- If implemented, over 20,000 computer science graduates a year across 100 UK universities to be taught cybersecurity to fill drastic national skills shortage.

London, UK, 30 June 2015: Universities now have access to the UK's first higher education cybersecurity learning guidelines for undergraduate degrees to be referenced within BCS, the Chartered Institute for IT, accreditation criteria for computing and IT-related degrees. Published by (ISC)^2, the largest not-for-profit membership body of certified information and software security professionals with nearly 110,000 members worldwide, and the Council of Professors and Head of Computing (CPHC), the guidelines reflect broad consultation with more than 30 universities and industry bodies. Developed in support of the UK government's National Cybersecurity Strategy, the guidelines define cybersecurity imperatives and learning outcomes affecting the next wave of computing degrees from as early as September 2015.

Matthew Hancock, Minister for the Cabinet Office said, "The UK has a world-class cybersecurity sector, but we can only continue in this vein if we have the highly skilled workforce we need to thrive. Initiatives, such as this, are excellent examples of encouraging the best young people to consider careers in cyber."

This ground-breaking effort means that over 100 UK universities will benefit from specific guidance for embedding and enhancing relevant cybersecurity principles, concepts and learning outcomes within their curricula at all levels. Students can be taught a broad spectrum of cybersecurity concepts, from threats and attacks to designing secure systems and products to governance based on up-to-date industry expertise.

The aim is to bring computing degrees into closer alignment with industry requirements. This effort could see over 20,000 graduates a year entering the UK workforce with the cybersecurity understanding and knowledge necessary to securely build the digital future and the IT infrastructure upon which the UK economy relies. Directly addressing objective four of the Government's National Cyber Security Strategy: "to equip the UK to have the cross-cutting knowledge, skills and capability it needs to underpin all our cybersecurity objectives", the initiative will also address a severe skills shortage by introducing more people to the opportunity of pursuing a career within the cybersecurity profession.

"This marks a significant shift in the teaching of security in higher education; cybersecurity is now being recognised as integral to every relevant computing discipline from computer game development to network engineering. Previously, cybersecurity was treated as a separate discipline to computing with students being taught how to create applications or develop systems and technology but not how to secure them; leading to proliferation of systems with built-in vulnerabilities," said **Carsten Maple, professor of Cyber Systems Engineering at University of Warwick and vice chair of the Council of Professors and Heads of Computing.** "Academia, industry and government have all recognised this, which is why we have come together to address this issue and provide a practical and accessible way of incorporating cybersecurity into our curricula, and move the discipline forward."

"The UK has long been affected by both a cybersecurity talent shortage and a mismatch between the capabilities of computing graduates and the requirements of industry. These compounding issues have ultimately been compromising our ability to both build and defend the digital economy and UK plc," said **Dr. Adrian Davis, CISSP, managing director for EMEA at (ISC)^2**. "We are now amongst the first nations in the world to ensure that cybersecurity will be embedded throughout every relevant computing degree and, crucially, the most up-to-date skills will be taught as the framework is built and maintained with the input of front-line information and cybersecurity professionals. UK graduates entering the workforce will be able to immediately put their skills to use."

(ISC)^2's recent Global Information Security Workforce Survey, the largest ever conducted with nearly 14,000 global respondents, found that 63 percent of UK public and private sector organisations have too few cybersecurity workers. One in five UK respondents admitted they would take over eight days to rectify a security breach.

"As an Institute we are already heavily involved in tackling the skills gap in this field; from developing the profession through to ensuring that standards are met," **Bill Mitchell, Director of Education at BCS,** explains. "This latest initiative means that additional guidance on cybersecurity elements will be provided to complement the existing information security criteria for computing-related degrees accredited by the BCS. Building cyber security into UK computing degree courses will go some way to resolving the skills gap situation by helping students to develop the skills that employers need."

The new "Cybersecurity Principles and Learning Outcomes" guidelines document was developed over two years throughout a series of workshop consultations with leading experts. These workshops included industry bodies such as the Institution of Engineering and Technology and Tech Partnership UK, government departments including the Cabinet Office and the Department for Business Innovation and Skills; and more than 30 universities that offer undergraduate computing science degrees from the newest post-92 universities to the Russell Group.

Supporting QUOTES:
Dr Alastair Irons, Head of Computing at the University of Sunderland and Chair of the BCS Academic Accreditation Committee said, "At the recent revalidation of its computer science suite of programmes the University of Sunderland embraced the CPHC (ISC)^2 workshop outcomes by embedding cybersecurity throughout the programmes and modules. The revalidated programmes give students the opportunity to develop knowledge and skills in the fundamentals of computer security and apply computer security principles across the curriculum for example defensive programming in programming, security design in database modules. In final year there is a new advanced cybersecurity module which is core for computer science and computer forensics students and available as an option module across the rest of the computer science suite."

Hugh Boyes, CEng, FIET, CISSP, Cyber Security Lead at the Institution of Engineering and Technology, said, "The development of these principles and learning outcomes facilitated by (ISC)^2 is an important step forward in improving the software security and thus the overall cybersecurity of systems. It is important that education providers address these principles and outcomes so that our future software engineers are better equipped to address the vulnerabilities that are so often prevalent in deployed software."

“Cybersecurity is a fundamental aspect of computing in the modern world, and we need to be sure that computing courses are being taught with security from the offset,” said **Nick Savage, Head of the School of Computing, University of Portsmouth**. “The key to the cybersecurity guidelines is that content will be integral to computing courses and not just a module added on. This should be reflected in the knowledge our graduates receive; application to operating system design will all be taught securely with cybersecurity implications at the front of mind. This is an important step change in the approach to cybersecurity education in the UK and we all need to be on board.”

“The employers of the Tech Partnership believe that cyber security awareness should be an integral part of every digital degree,” said **Dr. Tony Venus, Head of Standards at the Tech Partnership Company**, “and the new guidelines, developed in close collaboration with (ISC)² and BCS, will help universities implement this. The Tech Partnership is leading the way by actively incorporating the guidelines into its own degrees, including IT Management for Business; Software Development for Business; and the innovative new Degree Apprenticeship in Digital and Technology Solutions, which has core cybersecurity content as well as a cybersecurity specialist route.”

Guidelines Summary:

The development of the guidelines document was led by (ISC)² and CPHC over the last two years, and BCS provided the accreditation framework. The group also included cybersecurity professionals from the Russell Group Universities, Cabinet Office, MoD and the Institute of Engineering and Technology. Students will be taught an array of core concepts and principles, including:

1. **Information and risk:** models including confidentiality, integrity and availability (CIA); concepts such as probability, consequence, harm, risk identification, assessment and mitigation; and the relationship between information and system risk.
2. **Threats and attacks:** threats, how they materialise, typical attacks and how those attacks exploit vulnerabilities.
3. **Cybersecurity architecture and operations:** physical and process controls that can be implemented across an organisation to reduce information and systems risk, identify and mitigate vulnerability, and ensure organisational compliance.
4. **Secure systems and products:** the concepts of design, defensive programming and testing and their application to build robust, resilient systems that are fit for purpose.
5. **Cybersecurity management:** understanding the personal, organisational and legal/regulatory context in which information systems could be used, the risks of such use and the constraints (such as time, finance and people) that may affect how cybersecurity is implemented.

The full university guidelines can be found here: http://cert.isc2.org/isc2-cphc-whitepaper/

About (ISC)²

Formed in 1989, (ISC)² is the largest not-for-profit membership body of certified information and software security professionals worldwide, with nearly 110,000 members in more than 160 countries. Globally recognized as the Gold Standard, (ISC)² issues the Certified Authorization Professional (CAP®), Certified Cyber Forensics Professional (CCFP®), Certified Cloud Security Professional (CCSP℠), Certified Information Systems Security Professional (CISSP®) and related concentrations, Certified Secure Software Lifecycle Professional (CSSLP®), 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.

# # #

PR contact:
Proof Communication
Amita Hanspal
+44(0)20 8816 8002
amita@proofcommunication.com