Advancing and teaching cybersecurity skills for policing  
Dr Dianne Van Hemert, TNO, Human Behaviour and Organisational Innovations

The digital society poses different types of challenges to the police force. For example, police forces need detailed understanding and knowledge of cybercrime in order to more effectively perform their patrolling and investigating roles; they need insight into psychological profiles and vulnerabilities of victims of cybercrime, cybercriminals, and their own police staff; they need to be aware of the potential threats they are vulnerable to themselves. Addressing these challenges, we propose a tailor-made approach to advancing and teaching cybersecurity skills of police personnel. To adequately train police officers, the training should be preceded by a screening or profiling of skills, needs, and vulnerabilities. This way we can provide custom-made training solutions in terms of both content and format. The presentation will outline our tailor-made approach and illustrate by providing examples of recent projects.

Embedding Cybersecurity in the Computer Science Curriculum  
Professor Alastair Irons, Harjinder Singh Lallie, University of Sunderland

The aim of this paper is to present the findings from a project on integrating Cybersecurity into the Computer Science curriculum in Higher Education programmes. In 2013, an initiative was set up by (ISC)², CPHC and the Cabinet Office to examine embedding Cybersecurity into undergraduate Computer Science degrees. A series of workshops were held throughout 2013 and 2014 and the output from these was a set of principles focussing on Cybersecurity education and a framework for embedding these principles in UK Computing Science curricula. This paper provides a reflection on the implementation workshops held in March / April in 2016. The principles and framework were discussed at the workshops and examples of how two Universities had included Cybersecurity in CS curricula were shared. This paper presents a summary of the discussions, highlighting opportunities and challenges and concludes with an indication of the next steps in taking the agenda forward.

Towards a comprehensive cyber security learning and teaching strategy  
Dr Alexeis Garcia-Perez, Coventry University

There is a growing understanding of the complex nature of the cyber security ecosystem across management boards, individuals and groups. A valid cyber security strategy is one that enables visibility of external threats and vulnerabilities throughout a digital infrastructure whilst also enabling understanding of potential impact of an attack and effective ways of identifying and remediating it. With this shift in mindset, cyber security learning and teaching strategies need to combine knowledge of the technical infrastructure formed by applications, systems and networks, with that of their relationship with people and business processes. This paper describes how Coventry University understands and addresses the skills shortage in all areas of cyber security by covering the different dimensions of this subject in a learning and teaching strategy based on a range of cyber security programmes and a variety of methods designed to suit the needs of the different stakeholders.
Gamified Virtual Training Environment for Attacker-centric Cyber-security Skills Development
Dr Chitra Balakrishna, Edge Hill University

The findings of the latest cyber security status report by ISACA indicates the shortage of cyber-security professionals is universal and ongoing. A further study conducted by the Ministry of Universities and Science has identified a skills gap that exists amongst the fresh cyber-security graduates, who often do not possess the ability to apply their skills to real-world scenarios as employers demand. Effective cyber-security education unlike most other technical subjects not just requires a hands-on, real-world learning environment but also demands a change of behaviour amongst the learners.

CyberGaTE, the HEA funded project aims to bridge the skill-gap between theory and practice as well as address the specific needs of effective cyber-security training through innovative pedagogical practices such as gamification, attacker-centric challenge-based learning.

The Cyber Security Knowledge Exchange: Working with Employers to produce authentic PBL scenarios and enhance employability
Dr Chris Beaumont, Edge Hill University

This paper shares an approach used in the HEA Cyber Security Knowledge Exchange project funded as part of the HEA Learning & Teaching in Cyber Security Programme. The project uses innovative approaches, working with students and employers as partners to create On-line Problem-based Learning (PBL) Scenarios and resources for learning Cyber Security. Content is provided by employer partners to ensure relevance and authenticity.

The project also evaluated a student focussed Knowledge Exchange (KE) model of disseminating good cyber security practice to SMEs through work placements for MSc InfoSec students. As the project developed, it became clear that a consistent consulting and learning framework was needed to underpin the scenarios and models, and this is an additional project output.

The aims of the session are to:
• Critically discuss the project;
• Identify key messages and lessons learned from the project;
• Discuss how other organisations may adapt and use the materials or the approach.

A modular framework for building vulnerable systems for teaching computer security: randomised and parameterised hacking scenarios
Dr Z. Cliffe Schreuders, Leeds Beckett University

Computer security students benefit from engaging in hacking challenges. However, developing hacking challenges can be time consuming, and once created, essentially static. That is, once a challenge has been "solved" there is no remaining challenge for the student, and if the challenge is created for a competition or assessment, the challenge cannot be reused without risking plagiarism, and collusion. We have developed a unique solution: a platform for generating randomised vulnerable systems, Security Scenario Generator (SecGen). SecGen generates VMs based on a scenario specification, which describes the constraints and properties of the VMs to be created, such as vulnerabilities and services present. This presentation describes SecGen and the recent advances in it's design (currently being developed as part of a HEA funded project), namely its newly easily extendible modular and parametrised framework and how vulnerabilities and scenarios are specified.
Defence Against the Dark Arts: A University Wide Module to Educate the Masses  
Dr Natalie Coull and Dr Jackie Archilbald, Abertay University

The Cybersecurity Research Group at Abertay University have delivered a university-wide elective module on Cybersecurity to 1st year students across a range of disciplines including law, computer games, sports science and psychology students. In this presentation we will discuss the challenges of teaching cybersecurity to non-technical students, the benefits of educating the masses and we will also present our findings from a survey which assesses the impact of the module on the students’ online behaviour and cybersecurity practices.

An Edutainment-based Model for Design of ‘Taster’ Sessions to Raise Cybersecurity Awareness amongst School-leavers  
Mr David Chadwick, University of Greenwich

The Cyber Security Strategy 2011 voiced concern over lack of UK cyber-security training and awareness and outlined a particular goal: ‘encourage, support and develop education at all levels’. ‘At all levels’ implied IT novices, the median skilled and highly-skilled. In addition to expanding degree and research programmes, universities have seen a rise in cybersecurity ‘awareness-raising’ outreach to schools, employability exhibitions, and short courses for businesses where short-duration, maximum-impact, highly topical learning was required without prior knowledge, formal curriculum or assessment. As ‘awareness-raising’ sessions began to increase in number it was decided that a ‘model approach’ be created as a guide to tutors designing such sessions. This model, based upon edutainment (education + entertainment) methods has been trialled successfully in open-day ‘taster’ sessions for applicants to undergraduate cybersecurity degrees.

Professor William Buchanan, Edinburgh Napier University

This paper outlines the implementation and evaluation of the DFET Cloud for Cyber Security training and in the implementation of the Virtualised Security Operation Center [vSoC] project. [vSoC] uses state-of-the-art systems, software, tools and scenarios to create real-life networked infrastructures, which can be used for a range of Cyber Security training courses. This includes the creation of a virtualised SoC, and which integrates alerts from a real-life networked infrastructure, and the evaluation of the Cloud infrastructure over two years.

Enhancement Techniques for Student Engagement in Cybersecurity Education  
Mr Oliver Bill and Dr Basel Halak, University of Southampton

In order to create successful cybersecurity professionals, it is important to engage students in a way that bridges the gap from the academic to the real world. In this paper, we present three examples used within teaching at Southampton University: The use of real-world scenarios presented through virtual environments, the creation of a cryptography learning platform and the fostering of student communities to support learning through social networking.

We explore the ways in which practical hands-on experience based on industry can better support the development skills. We examine how real-life techniques can be combined with gamification and personalised learning to engender positive engagement. We consider how real-world scenarios within the educational institution can be utilised to further learning within in a safe but relevant context, being mutually beneficial to the students and institution. Finally, we consider the role of fostering a strong cybersecurity student community, using social networking, student societies and extra-curricular activities.
Practice-Informed Theory and Activity-Led Learning for Ethical Hacking
Dr James Shuttleworth, Coventry University

In the presented paper, we will explain the methods we have developed to teach ethical hacking and cybersecurity in a way that reinforces theoretical underpinnings while capitalising on the opportunities for practical work in the area. We explain how we believe that the combination of breadth and depth required by people who work in the field is difficult to meet at level 1, but also that the challenge is worth overcoming because of the benefits for enthusing students and embedding scaffolding that are called upon even in the in the final year of the programme.

Manual Games for Cyber Education: A Defence Academy of the UK experience
Major Tom Mouat, The Defence Academy of the UK

The aim of this session will be to discuss the experience of using the application of manual gaming techniques to cyber education within the Defence Academy of the UK. There is clear evidence that didactic lecture techniques are especially ineffective in the area of cyber education and that on-line learning, while adequate at explaining low level and individual security aspects, fail to cover the holistic aspects of the cyber threat that are of particular importance to senior leaders and business managers. The Defence Academy of the UK has been experimenting with manual gaming as an educational tool to complement existing learning delivery. This session will cover two different techniques and discuss the advantages & disadvantages in relation to educational outcomes.

Cybersecurity Teaching and Learning – Bridging the Gap between Current Awareness and Future Orientated Needs in Social Computing and Social Media
Dr Neil Gordon, University of Hull

This paper provides a snapshot of current awareness of online privacy and security amongst undergraduate and postgraduate students. It considers ways of moving forward from their current appreciation of cybersecurity towards a future orientated cyber-security aware culture. The paper starts builds from empirical foundations to discuss developments employing virtual learning environments and in particular MOOC solutions. The empirical data resulting from a survey of undergraduate and postgraduate masters students from differing disciplines, namely Computer Science and Media and Communications Students. The contrasting technical background enables a broader review of issues and comparison of differing needs. The survey focused on explicitly on online privacy, and implicitly on cybersecurity. Having established the issues, the paper then discusses how these inform the curriculum, including broader social impact and professional needs for computing specialists becomes critical, and outlines flexible and technology-enabled approaches to teaching this.

Security programming with high-level abstractions: a tutorial
Dr Paolo Modesti, University of Sunderland

The specification of security protocols with high-level programming abstractions, suited for security analysis and verification, has been advocated by the formal methods for security research community. Based on these principles of application design, we developed a tutorial to introduce undergraduate students to the foundations of security programming. The main pedagogical goal of this tutorial is to teach, in a simple and effective way, how to build secure distributed applications using common cryptographic primitives abstracting from their low-level details. The tutorial is aimed at helping the students to quickly grasp the main security concepts and to effectively apply them to the coding of distributed programs implementing security properties like authentication and secrecy. As programming is one of the main skills required by the cybersecurity industry, we believe that this tutorial can contribute to the professional development of future graduates.
A forward-looking Digital Forensics curriculum design to meet emerging market challenges
Dr Syed Naqvi, Birmingham City University

This session will provide a discussion platform for sharing experience of upgrading Digital Forensics curriculum to provide required digital investigation skills to our students and as a result to meet employer expectations. An overview of the emerging landscape of Cyberspace will be provided together with the challenges of investigating its artefacts. A set of industrial requirements will also be presented to help develop a rationale for our proposed future-oriented Digital Forensics course. Various modules of this course and their positioning will be presented. Participants will be actively engaged, and encouraged to provide their opinion and experience of developing similar teaching modules and discussing ways of overcoming any constraints that may be encountered. This session will also provide an opportunity to share experience of running similar highly-dynamic professional courses. This will include among others: identification of new industrial requirements, selection of appropriate learning activities, stakeholder feedback, and accreditation issues.

Virtualising the Digital Crime Scene & Cyber Security Breach – A new generation for gamification in identifying the digital artefact
Mr Adrian Winckles, Anglia Ruskin University

In this session we will introduce VDECS, a Virtual Digital Evidence Crime Scenes application that offers an accessible, configurable, incident scene simulation for digital forensic/cyber security incident training within a gamification/e-learning framework. VDECS develops and evaluates pedagogic practice, meeting the needs of a diverse student base (cyber security/forensic/crime enforcement professionals). The application provides scenarios, interactive objects and student transcripts that can be accessed via a web interface to allow tutors to configure crime scenes and provide feedback and feedforward.

The project proposes a cloud computing platform where participants can make contributions, share applications, use and evaluate resources; allowing wide community engagement with minimal investment in infrastructure.

Using open source intelligence techniques to highlight the dangers of an open social media profile.
Mr Ronnie Smyth, De Montfort University

There is increasing concern over the amount of personal information that people are openly willing to share on social media platforms (Gross R, 2005). This information is gathered and used against targets in complex social engineering attacks (Mann P, 2012). It has been found that with no prior training a student is able to find a significant amount of information that can then be developed into an attack. Through highlighting the ease with which this information is collected, processed and then developed into attacks it is shown that it has a direct effect on the students own use of social media. This was found to be especially successful when the lecturer put themselves forward as a target, meaning the students have a personal attachment to the target (Cialdini R.B., 1987). This paper examines the task set to all students, analyses the information discovered by the students and considers the overall effect on the students themselves.
Extending the Reach of Cyber Security Through Supported Online Learning
Mr Robert Wraith, NCG Direct

This session will be presented in two parts covering the details in relation to the conclusion of the Cyber Security project ‘Active Cyber Security Learning in a Vocational Setting’ which was completed by the Digital Skills Academy and supported by both the HEA and the Department for Business, Innovation and Skills.

The second part of the presentation will deliver the details relating to the further development of this Cyber Security programme with NCG Direct – Supported Online Learning. It will demonstrate the software that is used and demonstrate how and why we have developed new and innovative ways in which to continue to bridge the gap between the academic and working world by reaching out to those learners who are unable to attend conventional courses within a University or College environment around the world.

Enriching the Student Cyber Security Experience with the University Challenge
Mr Adrian Winckles, Anglia Ruskin University

For students studying cybersecurity related courses there is often a dichotomy between the theory of their studies and the practical implementation of the knowledge and skills earned. In a never competitive employment marketplace, it is no longer enough to be able to say “I’ve a 2:1, employ me”, the potential employer is looking for additional “value added” experiences that differentiate the candidates.

Within degree courses there is a need to build a sense of community with the student cohort by offering the engagement with extracurricular activities and meeting the aspirations for increasing the student’s employability prospects.

Universities serious about giving students real life experience and encouraging engagement in the Cybersecurity industry should think about teams to engaging in "hacking" competitions and "capture the flag" events.

How can university/industry communities of interest come together, capture the spirit of these types of challenges to benefit the student community and industry engagement?

Cyber Security Teaching and Learning: Information Assurance Auditing Platform
Mr Jonathan Barlow, Liverpool John Moore’s University

Cyber security is becoming a greater concern for today’s society, with attacks on systems now being a daily occurrence for many businesses and governments alike. I have noticed a divide and a clear evident skills gap within the teaching and learning of cyber security. This gap is also noted by many of the leading cyber security experts across the world who are striving for a solution to this problem. A practical hand on approach for student learning is centric to the development of future cyber security experts and is where an environment that is safe for students to apply practical skills is needed. Cyber Security Teaching and Learning: Information Assurance Auditing Platform.

The aim of the session would to explain current flaws in the cyber security teaching and learning program and why a practical environment is needed. Also demonstrate a virtual environment that has been explored within my project and how that can be developed.