CYBER 22-26 APRIL
SCOTLAND
WEEK 2019

College Development Network | Leading Creating Sharing

College Cyber Security Conference

Tuesday 23 April 2019

Stirling Court Hotel, University of Stirling, Stirling, FK9 4LA

In partnership with:

Scottish Government
Riaghaltas na h-Alba
gov.scot

#CyberScotWeek19

Programme

0930 **Registration and Coffee**

1000 **Welcome and Introductions**
Jim Metcalfe, Chief Executive, CDN

1005 **Ministerial Address**
Kate Forbes MSP, Minister for Public Finance and Digital Economy

1015 **Developing the Cyber Pipeline**
Chelsea Jarvie, Security and Information Risk Manager, The Scottish Government

With the development of new qualifications in cyber security and a growing demand for specialists in the public and private sectors, colleges are well-placed to attract a new cohort of future cyber specialists. It's also an opportunity to encourage more women into cyber, as the numbers of women joining the field increase.

1045 **Workshop Session One**

Delegates should select one of the three workshop sessions available at this time to attend. Further information on workshops can be found below.

Please note that the Table Top Scenario Testing session has limited availability and is specifically targeted at senior college staff and board members.

1130 **Coffee**

1145 **Workshop Session Two**

Delegates should select one of the three workshop sessions available at this time to attend. Further information on workshops can be found below.

Please note that the Table Top Scenario Testing session has limited availability and is specifically targeted at senior college staff and board members.

1230 **Lunch**

1315 **Are Colleges the Unrecognised BFG of the Cyber World?**
Dr Martin Beaton, Scottish Cyber Cluster Expert

Remember the BFG from the first-person shooter game “Doom” in the 90s? In this presentation we will explore how colleges, largely ignored in the cyber skills struggle, could in fact be the biggest and best tool for producing talent at the scale Scotland needs.

1335 **Managing Personal Cyber Security Risk**
Gary Ennis, NSDesign

“The biggest thing you can do to protect against the risks of cyber security, is to better educate yourself and your staff.” With everyone and their dog (literally) using Social Media, this fast and furious workshop will explore the legalities, cyber risks, business threats and more. From social engineering to social faux-pas, we take a fun look at idiots being idiots and give a reminder not to be one!

1410 **“Hello, 999. Police? No. Fire? No! Cyber Service, Please!”**
Dr Marwan Fayed, Senior Lecturer, University of St Andrews; Co-founder and Director of HUBS c.i.c.

So many incident reports; so much guidance; so much that it’s easy to feel insecure, even frightened. Who do we call? What do we do? Yes, there are risks. Indeed, the way forward is often unclear, so are the guidelines. The truth is, we’re all in this together. The most important things are no so different from those we already know.

1440 **Comfort Break**

1445 **The Big Data Show**

The Big Data Show combines digital gaming with live performance to tell the story of the first prosecution of hackers in the UK. An enthralling, entertaining, interactive experience, the Big Data Show threads the story of that very first headline hack in 1984 through the modern experiences of life online. The show combines storytelling with mobile gaming and big data tech to demystify online privacy, data security, and staying safe in a virtual world asking: what might it mean to be a digital citizen?

1545 **Roundup of the Day**
Jim Metcalfe, Chief Executive, CDN

1600 **Close**

Workshop Session One

Workshop A	**Staying Safe in a Digital World** Eamonn Keane, Head of Cyber Security & Innovation, Scottish Business Resilience Centre Ltd. + Ethical Hacker, Abertay University Learn about the practicalities of cyber security as Eamonn and an Ethical Hacker from Abertay University describe the cyber threat landscape and the steps you and your students need to take to remain safe in a digital environment.
Workshop B	**Security Maturity Model for Efficient Planning and Risk Reduction** Jordan Schroeder, HEFESTIS Ltd. There are many things that an institution can do to improve information security, but it can be difficult to determine what should be prioritised. Without a clear method to prioritise, an institution chases the biggest threat of the moment or whatever generic framework an external auditor has suggested. This results in inefficient information security programme that may or may not address the actual risks of the institution. By using a Maturity Model approach, the institution can focus on the highest impact areas in the right level of effort and measurably reduce risks.
Workshop C	**Table Top Scenario Testing** Terry Trundley, UCSS Epidemic; building fire; bomb threat; extreme weather - your Business Continuity and Disaster Recovery (BC DR) Plan will address all these scenarios. However, when it comes to cyber resilience, many organisations expect the IT department to deal with the response to any business-critical events. This is a very high-risk approach. To find out what the board and senior management team should be considering within the cyber resilience section of the BC DR Plan, this session will take you through a real scenario with some fascinating and revealing insights. Whether cyber issues are already incorporated into your BC DR Plan or not, you will come away with a highly practical sense check for your institution's cyber resilience approaches.

Workshop Session Two

Workshop D	**Employer Perspective: Panel Session** Chaired by Dr Martin Beaton
Workshop E	**National and Higher National Qualifications in Cyber Security** Bobby Elliott, SQA and Joe Harkins, West College Scotland Hands-on session with support materials for NPA Cyber Security, explore HNC Cyber Security and contribute to the development of HND Cyber Security.
Workshop F	**Table Top Scenario Testing** Terry Trundley, UCSS Epidemic; building fire; bomb threat; extreme weather - your Business Continuity and Disaster Recovery (BC DR) Plan will address all these scenarios. However, when it comes to cyber resilience, many organisations expect the IT department to deal with the response to any business-critical events. This is a very high-risk approach. To find out what the board and senior management team should be considering within the cyber resilience section of the BC DR Plan, this session will take you through a real scenario with some fascinating and revealing insights. Whether cyber issues are already incorporated into your BC DR Plan or not, you will come away with a highly practical sense check for your institution’s cyber resilience approaches.