Executive Education Certificate

in Cyber Security for Public and Private Sector Organisations

Scottish Business
Resilience Centre

Security.

Executive Education Certificate.

In today's landscape of escalating cybercrime, mitigating cyber risk is not the Chief Information Security Officer's responsibility alone — it is everyone's job. Getting ahead of hackers and other security risks requires the active engagement of non-technical management, as well as an overall commitment to building a cyber security culture within your organisations.

This programme provides CEO's. Directors and Non-Exec Directors with frameworks and best practices for managing cyber security-related risk separate from the specialized IT infrastructure typically associated with this topic. Course content includes lectures, highly interactive discussions, and case studies related to:

- Cyber security awareness
- Non-tech leader's role in cyber security management
- Actionable ideas to increase your organisation's cyber resilience
- Measuring your organisation's cyber-safety level - and how this changes over time
- How to speak the language of cyber security - enable informed conversations with your technology teams and colleagues, and ensure your organization is as cyber secure as possible

Module 1:
The Internet: understanding how it works

- History of the Internet — from academic experiment to global connectivity
- The physics and engineering of the Internet
- Today's landscape - overview of the Internet, World Wide Web and beyond

Modern communications

- Computer networks
- Mobile telecommunications: From 1G to 5G
- The Internet of Things

Joining the dots

- Understanding the applicability to your organisation
- How does this tie into cyber security?
- Being able to ask the right questions

Module 2
Cyber Security — what's all the fuss?

Two half day sessions with case study work outside of the programme in groups.

A brief history of Cyber

Key concepts in Cyber Security

- Vulnerabilities and exploits
- Data exfiltration, disruption, ransomware, prepositioning

The theory behind hacking

- Why do people do it?
- Hacking Demo

Cyber attacks

- How basic and advanced cyber attacks work
- What harm can they do?
- Nation states, criminals and why terrorists don't do cyber

How attacks affect organisations

- Loss of money, IP and data
- Strategic disadvantage: espionage, prepositioning and political interference
- Disruption and actual harm

Hands on hacking activity

Module 3:
Managing cyber security risk

Cyber Security as an organisational risk

The key concepts of confidentiality, integrity and availability of data and infrastructure

Setting a risk threshold: the 'Crown Jewels' Concept

The technical aspects:

- Perimeter defences
- Anomaly detection (the Snowden example of what can be stolen when you don't do this)
- The role of threat intelligence

The human aspects

- People are not the weakest link: making technology easier to use safely
- Passwords
- Clicking on dodgy links
- Safe and secure homeworking

Incident Management: the importance of non-technical factors

- Resilience and backups
- communications

Executive Education Certificate.

The programme is designed and delivered by Professor Ciaran Martin and Declan Doyle.

Ciaran Martin is Professor of Practice in the Management of Public Organisations.

Prior to joining the School, Ciaran was the founding Chief Executive of the National Cyber Security Centre, part of GCHQ.

Ciaran led a fundamental shift in the UK's approach to cyber security in the second half of the last decade. He successfully advocated for a wholesale change of approach towards a more interventionist posture and this was adopted by the Government in the 2015 National Security Strategy, leading to the creation of the NCSC in 2016 under his leadership. Over the same timeframe, the UK has moved from joint eighth to first in the International Telecommunications Union's Global Cyber security Index and the NCSC model has been studied widely and adopted in countries like Canada and Australia. The NCSC's approach has been lauded for responding quickly to incidents and giving the British public clear and prompt advice on responding to them, putting previously classified information in the hands of industry so that companies can defend themselves more effectively, major improvements in automatic cyber security like countering brand spoofing and rapidly taking down malicious sites, and projecting the UK's leadership in cyber security across the world. Ciaran's work, which led to him being appointed CB in the 2020 New Year's Honour's list, has also been recognised and honoured in the United States and elsewhere across the world.

In his 23-year career in the UK civil service, Ciaran held senior roles within the Cabinet Office, including Constitution Director (2011-2014), which included negotiating the basis of the Scottish Referendum with the Scottish Government and spearheading the equalising of the Royal Succession laws between males and females in the line; and director of Security and Intelligence at the Cabinet Office (2008-2011). Between 2002 and 2008 he was Principal Private Secretary to the Cabinet Secretary and Head of the Civil Service and Private Secretary to the Permanent Secretary to HM Treasury.

As well as secure technology, a constant theme has been the promotion of responsible, values-based Government whether in the Treasury, Cabinet Office or the security services. As a native of Northern Ireland's troubles which he saw in part as being themselves caused by a failure of Government, Ciaran knows the importance of fair, impartial, well run public services that work for all and are trusted. So, prior to his NCSC career he is particular proud of his supporting role, along with Ministers and civil servants in London and Edinburgh, in framing the arrangements for the 2014 independence referendum an event which, whilst hotly contested, was seen by all to be fair, legally sound and decisive. His knowledge of public finances, national and international security and the central bureaucracy of Whitehall is a rare combination of experiences and expertise.

Declan Doyle is Head of Ethical Hacking at SBRC.

Declan has spent his life immersed in cyber and is passionate about ensuring companies build both strong cyber security practices and positive cyber security culture.

As Head of Ethical Hacking, Declan is responsible for delivering a wide range of cyber services and support that SBRC offers, whilst also managing SBRCs cohort of Ethical Hacking students. He is lead facilitator for the Exercise in a Box project, a Scottish Government funded project aimed at spreading awareness for the National Cyber Security Centre (NCSC) designed tool. Declan initially joined SBRC many moons ago as one of the Ethical Hacking students studying at Abertay University, regarded as an Academic Centre of Excellence in Cyber Security Education by the NCSC. He has experience in delivering an extensive range of cyber services, from vulnerability assessments to phishing campaigns, and has worked with companies of all sizes and sectors, from Fortune500 to startups.

He is an advocate of promoting STEM skills to the younger generation and is an active mentor and coach to the next generation of cyber security professionals in Scotland.

There will be 3 modules delivered online over 4 sessions during March/April 2021

- **Monday 8 March: 9:30 to 12:30**
- **Thursday 25 March: 17:00 to 19:30**
- **Monday 12 April: 9:30 to 12:30**
- **Thursday 22 April: 17:00 to 19:30**

Places will be allocated to CEO/Director level or equivalent in public sector only.

Places are limited to 30 and are non-transferable.

This programme is free of charge to attend and funded by Scottish Government.

Future dates will be added. There will be up to 5 cohorts.

To apply for a place on this, or a later cohort, please click here to register.

Scottish Business Resilience Centre