CYBER SECURITY TECHNOLOGIST HIGHER APPRENTICESHIP

Level:

4

Duration:

24 Months - One day training per fortnight

Entry requirements:

Individual employers will set the selection criteria, but this is likely to include A' Levels, a relevant Level 3 apprenticeship, or other relevant qualifications, experience and/or an aptitude test with a focus on functional skills level 2 in maths and English.

Overview:

The primary role of Cyber Security Technologist is to apply an understanding of cyber threats, hazards, risks, controls, measures and mitigation to protect organisations systems and people. Those who choose the technical side of the apprenticeship will focus on areas including security design & architecture, security testing, investigations & response. Those focussed on the risk analyst side will concentrate on areas such as operations, risks, governance & compliance. All people in this occupation work to achieve required security outcomes in a legal and regulatory context in all parts of the economy. They develop and apply practical knowledge of information security to deliver solutions that fulfil an organisation's requirement.

Aim:

TECHNICAL KNOWELDGE AND UNDERSTANDING FOR THE CORE UNITS

Understands the basics of cyber security including:

1. Why cyber security matters – the importance to business and society
2. Basic theory – concepts such as security, identity, confidentiality, integrity, availability, threat, vulnerability, risk and hazard. Also how these relate to each other and lead to risk and harm
3. Security assurance – concepts (can explain what assurance is for in security, and 'trustworthy' versus 'trusted') and how assurance may be achieved in practice (can explain what penetration testing is and how it contributes to assurance; and extrinsic assurance methods)
4. How to build a security case – delivering security objectives with reasoned justification in a representative business scenario
5. Cyber security concepts applied to ICT infrastructure – can describe the fundamental building blocks and typical architectures and identify some common vulnerabilities in networks and systems.
6. Attack techniques and sources of threat – can describe the main types of common attack techniques; also the role of human behaviour. Explain how attack techniques combine with motive and opportunity to become a threat.
7. Cyber defence – describe ways to defend against attack techniques
8. Relevant laws and ethics – describe security standards, regulations and their consequences across at least two sectors; the role of criminal and other law; key relevant features of UK and international law
9. The existing threat landscape – can describe and know how to apply relevant techniques for horizon scanning including use of recognised sources of threat intelligence
10. Threat trends – can describe the significance of identified trends in cyber security and understand the value and risk of this analysis

SPECIALISMS

In addition to the core, all apprentices will do ONE of the following specialisms:

OPTION 1: TECHNOLOGIST

- Understand the basic of networks: data, protocols and how they relate to each other; the main routing protocols; the main factors affecting network performance including typical failure modes in protocols and approaches to error control.
- Understand at a deeper level than from Knowledge Module 1, how to build a security case: describe what good practice in design is; describe common security architectures; be aware of reputable security architectures that incorporates hardware and software components, and sources of architecture patterns and guidance. Understand how to build a security case including context, threats, justifying the selected mitigations and security controls with reasoning and recognising the dynamic and adaptable nature of threats.
- Understand how cyber security technology components are typically deployed in networks and systems to provide security functionality including: hardware and software.
- Understand the basics of cryptography – can describe the main techniques, the significance of key management, appreciate the legal issues

OPTION 2: RISK ANALYST

- Understanding relevant types of risk assessment methodologies and approaches to risk treatment, can identify the vulnerabilities in organisations and security management systems; understand the threat intelligence lifecycle; describe different approaches to risk treatment. Understand the role of the risk owner and contrast that role with other stakeholders.
- Understand at a deeper level than from knowledge Module 1, the legal, standards, regulations and ethical standards relevant to cyber security: governance, organisational structure, roles, policies, standard, guidelines and how they all work together to deliver identified security outcomes. Also awareness of the legal framework, key concepts applying to ISO27001 (a specification for the information security management), and awareness of legal and regulatory obligations for breach notification

Where Can I Study?

Training 2000 Blackburn

Method of delivery?

- Flexible delivery comprising of knowledge and tutorial workshops for one to one development and support
- One day classroom delivery every fortnight and work based learning
- Face-to-face tutorials
- Distance learning or study at our ‘state of the art’ Cyber Security Centre
- Opportunities to develop real life workplace projects with employers
- Assessor visits
- Access to learning on e-portfolio

Any other useful Information:

This apprenticeship is recognised for entry to both IISP and BCS Associate Membership and for entry onto the Register of IT Technicians confirming SFIA level 3 professional competence. Those completing the apprenticeship are eligible to apply for registration.

Date last updated: 15/08/2017