INSTITUTE FOR APPRENTICESHIPS

CYBER SECURITY TECHNOLOGIST

Reference Number: ST0124

Details of standard

Role Profile

The primary role of a Cyber Security Technologist is to apply an understanding of cyber threats, hazards, risks, controls, measures and mitigations to protect organisations systems and people.

Those focused on the technical side work on areas such as security design & architecture, security testing, investigations & response.

Those focussed on the risk analysis side focus on areas such as operations, risk, governance & compliance.

Whether focussed on the technical or risk analysis side, 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 requirements.

Typical job roles

Cyber Operations Manager, Security Architect, Penetration Tester, Security Analyst, Risk Analyst, Intelligence Researcher, Security Sales Engineer, Cyber Security Specialist, Information Security Analyst, Governance & Compliance Analyst, Information Security Assurance & Threat Analyst, Forensics & Incident Response Analyst, Security Engineer, Information Security Auditor, Security Administrator, Information Security Officer.

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, relevant experience and/or an aptitude test with a focus on functional maths.

Technical Competencies and Technical Knowledge and Understanding

CORE

ALL apprentices will cover the following:

Technical Competencies	Technical Knowledge and Understanding
Threats, hazards, risks and intelligence • Discover (through a mix of research and practical exploration) vulnerabilities in a	Understands the basics of cyber security including:

system

- Analyse and evaluate security threats and hazards to a system or service or processes. Be aware of and demonstrate use of relevant external sources of threat intelligence or advice (e.g. CERT UK). Combine different sources to create an enriched view.
- Research and investigate some common attack techniques and recommend how to defend against them. Be aware of and demonstrate use of relevant external sources of vulnerabilities (e.g. OWASP)
- Undertake a security risk assessment for a simple system without direct supervision and propose basic remediation advice in the context of the employer.

Developing and using a security case

- Source and analyse a security case (e.g. a Common Criteria Protection Profile for a security component) and describe what threats, vulnerability or risks are mitigated and identify any residual areas of concern.
- Develop a simple security case without supervision. (A security case should describe the security objectives, threats, and for every identified attack technique identify mitigation or security controls that could include technical, implementation, policy or process).

Organisational context

- Identify and follow organisational policies and standards for information and cyber security.
- Operate according to service level agreements or employer defined performance targets. Future Trends
- Investigate different views of the future (using more than one external source) and trends in a relevant technology area and describe what this might mean for your business, with supporting reasoning.

- Why cyber security matters – the importance to business and society
- -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
- 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)
- How to build a security case – deriving security objectives with reasoned justification in a representative business scenario
- 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.
- 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.
- Cyber defence – describe ways to defend against attack techniques
- 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
- The existing threat landscape – can describe and know how to apply relevant techniques for horizon scanning including use of recognised sources of threat intelligence
- Threat trends – can describe the significance of identified trends in cyber security and understand the value and risk of this analyss

SPECIALISMS

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

Option 1: Technologist

Technical Competencies

Design build & test a network ("Build a network")

- Design, build, test and troubleshoot a network incorporating more than one subnet with static and dynamic routes, that includes servers, hubs, switches, routers and user devices to a given design requirement without supervision. Provide evidence that the system meets the design requirement.

Analysing a security case ("Make the security case")

- Analyse security requirements (functional and non-functional security requirements that may be presented in a security case) against other design requirements (e.g. usability, cost, size, weight, power, heat, supportability etc.), given for a given system or product. Identify conflicting requirements and propose, with reasoning, resolution through appropriate trade-offs.

Structured and reasoned implementation of security in a network ("Build a secure network")

- Design and build a simple system in accordance with a simple security case. Provide evidence that the system has properly implemented the security controls required by the security case.The system could be either at the enterprise, network or application layer.
- Select and configure relevant types of common security hardware and software components to implement a given security policy.
- Design a system employing a crypto to meet defined security objectives.

Technical Knowledge and Understanding

- Understands the basics 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.
- Understands, 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.
- Understands how cyber security technology components are typically deployed in networks and systems to provide security functionality including: hardware and software
- Understands the basics of cryptography – can describe the main techniques, the significance of key management, appreciate the legal issues

Develop and implement a key management plan for the given scenario/system.

Option 2: Risk Analyst

Technical Competencies

Cyber security risk assessment

- Conduct a cyber-risk assessment against an externally (market) recognised cyber security standard using a recognised risk assessment methodology.
- Identify threats relevant to a specific organisation and/or sector. Information security policy and process
- Develop an information security policy or process to address an identified risk.
- Develop an information security policy within a defined scope to take account of a minimum of 1 law or regulation relevant to cyber security.

Audit and assurance

- Take an active part in a security audit against a recognised cyber security standard, undertake a gap analysis and make recommendations for remediation.

Incident response and business continuity

- Develop an incident response plan for approval (within an organisations governance arrangements for incident response).
- Develop a business continuity plan for approval (within an organisations governance arrangements for business continuity).

Cyber security culture in an organisation

- Assess security culture using a recognised approach.
- Design and implement a simple 'security awareness' campaign to

Technical Knowledge and Understanding

Understands 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.

Understands, 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 these all work together to deliver identified security outcomes. Also awareness of the legal framework, key concepts applying to ISO27001 (a specification for information security management), and awareness of legal and regulatory obligations for breach notificatio

address a specific aspect of a security culture.

Underpinning Skills, Attitudes & Behaviours

- Logical and creative thinking skills
- Analytical and problem solving skills
- Ability to work independently and to take responsibility
- Can use own initiative
- A thorough and organised approach
- Ability to work with a range of internal and external people
- Ability to communicate effectively in a variety of situations
- Maintain productive, professional and secure working environment

Qualifications

The Knowledge Modules are summarised below and further details are available in the occupational brief available from the Tech Partnership at https://www.thetechpartnership.com/apprenticeship/cybersecuritytechnologist

No vendor or professional qualifications have been identified that would exempt these Knowledge Modules. Core (all the apprentices take this Knowledge Module)

Knowledge Module 1: Cyber Security Introduction

AND

Option 1 (Technologist): in addition to the core

Knowledge Module 2: Network and Digital Communications Theory Knowledge Module 3: Security Case Development and Design Good Practice Knowledge Module 4: Security Technology Building Blocks

Knowledge Module 5: Employment of Cryptography

OR

Option 2 (Risk Analyst): in addition to the core

Knowledge Module 6: Risk Assessment

Knowledge Module 7: Governance, Organisation, Law, Regulation & Standards

English and Maths

Level 2 English and maths will need to be achieved, if not already, prior to taking the end point assessment.

Professional Recognition

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.

Duration

The duration of this apprenticeship is typically 24 months.

Level

This is a level 4 apprenticeship

Review Date

This standard will be reviewed in April 2017.
