THE APPRENTICE and TRAINING PARTNERSHIP

LEVEL 4
CYBER SECURITY TECHNOLOGIST

Programme Overview:

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.

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.

Initial Assessments:

An initial assessment of Maths and English will be carried out for all apprentices using an approved diagnostic tool (BKSB, ForSkills); this will include Initial Assessment and full Diagnostic of knowledge in Maths and English to gauge the level at which the apprentice is working. This will enable us to support the apprentice and structure training provision.

Who is it for?

Cyber Security Technologist Level 4 Standard may have key responsibilities which can include:

- 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

Programme Duration:

The duration of this apprenticeship is typically 24 months

Delivery Model

A minimum of 20% of the apprenticeship training takes place off-the-job and is flexibly delivered to suit your business with either classroom training and/or workshops in the workplace or block-training or day-release at our centre, with the remaining time being spent in the workplace.

A full timetable for training, ongoing assessment and End-Point Assessment will be issued to both you as the employer; and the apprentice, once the delivery model and training elements have been agreed.

On Programme Assessment will take the form of progress reviews with the trainer, employer and apprentice at least every 12 weeks. Feedback with ongoing development will include additional learning materials, resources and training delivered through the apprentice's e-portfolio OneFile; to which employers have access to view the progress and the development of each apprentice.

If you have any questions relating to this Apprenticeship Standard, please contact
Katie Fowler, Head of Operations and Quality **T.** 0330 380 0249 **E.** k.fowler@theatp.co.uk

End Point Assessment:

As the apprentice progresses through the apprenticeship, the employer and training provider will agree the apprentice has meet the Standard and be ready for End Point Assessment. This is called the 'Gateway' and will trigger End-Point Assessment.

This is carried out by a Qualified Independent Assessor by an Approved External Awarding Organisation and will test the knowledge and competencies of the apprentice using a range of methods, these can include; an interview, scenarios with questions, portfolio of evidence sampled, professional discussion, watching a presentation of the apprentice's evidence plus other methods.

The Independent Assessor will make the final judgement as to whether the apprentice has fully met the requirements of the Standard. Grading will also be awarded with a maximum mark of 100, this will be awarded by the Independent Assessor based on the apprentice's assessment. Grades awarded are distinction, merit, pass or fail. End-Point Assessment is normally carried out in the workplace.

Programme Structure:

The programme is broken down into areas to ensure that each apprentice has a rounded knowledge of principles, techniques and technologies. This involves an understanding of knowledge, skills and behaviour; as well as managing self and delivering results.

Technical Competencies

The programme is broken down into areas to ensure that each apprentice has a rounded knowledge of principles, techniques and technologies. This involves an understanding of knowledge, skills and behaviour; as well as managing self and delivering results.

- **Threats, hazards, risks and intelligence**
  Discover (through a mix of research and practical exploration) vulnerabilities in a 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. Recognises anomalies in observed network data structures (including. by inspection of network packet data structures) and network behaviours (including by inspection of protocol behaviours) and by inspection of log files and by investigation of alerts raised by automated tools including SIEM tools.

- **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.

Technical Knowledge and Understanding

Delivered through one to one training sessions, workshops and tutorials and applied according to business environment

- **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

- **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 analysis

If you have any questions relating to this Apprenticeship Standard, please contact
Katie Fowler, Head of Operations and Quality **T.** 0330 380 0249 **E.** k.fowler@theatp.co.uk

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

- **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

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 address a specific aspect of a security culture.

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 notification.

If you have any questions relating to this Apprenticeship Standard, please contact
Katie Fowler, Head of Operations and Quality **T.** 0330 380 0249 **E.** k.fowler@theatp.co.uk

Underpinning Skills, Attitudes and Behaviours

Learned through a blended mixture via on the job training and one to one training sessions, workshops and tutorials and applied according to business environment.

- 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.

The designated trainer will support the employer and apprentice throughout the programme as a single point of contact for questions and queries. This includes additional support for portfolio and project preparation, along with any advice and guidance needed.

Qualifications:

Core (all the apprentices take this Knowledge Module)

KM1: Cyber Security Introduction

AND

Option 1 (Technologist): in addition to the core

KM2: Network and Digital Communications Theory
KM3: Security Case Development and Design Good Practice
KM4: Security Technology Building Blocks
KM5: Employment of Cryptography OR

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

KM6: Risk Assessment
KM7: Governance, Organisation, Law, Regulation & Standards

Progression:

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.

Next steps:

In order to create an apprenticeship that best suits your business requirements, we will meet with you to discuss the delivery of the programme and how the apprenticeship will be funded. We will provide ongoing support including:

- Search and selection of the right apprentices to meet your business requirements.
- Specifying the training modules to optimise 'in job' performance.
- A tailored service in order to seamlessly integrate with your apprentice managers.
- Updates and information regarding apprenticeship costs and funding.
- Support and guidance for the apprentice and employer from start to finish with one main point of contact for you throughout the whole apprenticeship.
- Employer and apprentice access to a comprehensive range of resources and support material via OneFile.
- Time-efficient visits for training and assessment to work around you.
- Industry specialist qualified trainers and assessors.

Questions?

If you have any questions or concerns relating to supporting an Apprentice, your assigned tutor is always available to help, or, contact one of our advisors on **0330 380 0249.**

If you have any questions relating to this Apprenticeship Standard, please contact Katie Fowler, Head of Operations and Quality **T.** 0330 380 0249 **E.** k.fowler@theatp.co.uk