LEVEL 4 CYBER SECURITY TECHNOLOGIST

There is nothing standard about the new apprenticeship Standards!

Following the 2019-2021 digital skills review, modern apprenticeships have once again taken a leap forward to provide better vocational training for apprentices and greater benefit to employers. The perfect solution for new career starts, professional upskilling or changes in career direction.

Programme Overview:

There are three separate pathways available in this apprenticeship:

- Cyber Security Engineer
- Cyber Defend & Respond
- Cyber Risk Analyst

All pathways have common core elements taught followed by the specialisms defined in each pathway. The core and specialist details are all expressed over the next few pages.

An important point to note: Although the description of competencies taught throughout each pathway may appear similar in some instances, the context, perspective, depth and application will differ greatly according to the purpose of each pathway.

Entry Requirements:

Entry requirements exist for all funded Further Education programmes. These ensure the value, gain and success of the programme. The ATP will conduct the processes with employers and prospective apprentices to determine correct funding eligibility.

Job role eligibility (known as Competency Role Map):

The job role must contain opportunity for an apprentice to practice the content set out in the apprenticeship Standard to achieve vocational competency. Apprentices must have the opportunity to practice the knowledge taught in training sessions in order to convert new knowledge in to sustainable skills applied in the workplace.

Each apprenticeship requires a portfolio of evidence, which will showcase the apprentice's work and will be reviewed by the End Point Assessment Organisation to determine how well new knowledge has been successfully utilised vocationally. If a job role is close to the eligibility criteria we will consult with employers to see if adjustments can be made to ensure the criteria is met.

Initial Assessment of existing knowledge and skills:

A prospective apprentice must stand to gain significant knowledge and skills from an apprenticeship. If the apprenticeship is too advanced for them or if they already know much of the knowledge and skills the apprenticeship would provide then they may not be eligible for the funding at Level 4 but might be well suited instead to the Level 3 Cyber Security Technician apprenticeship (details in a separate brochure).

The ATP will review existing qualifications, knowledge and skills to determine if the prospective apprentice will benefit from the proposed apprenticeship such that it meets the funding criteria. In most instances this is very straightforward, however in some instances funding can be specially authorised for reduction in order to fund the parts of an apprenticeship that would be relevant. The ATP will provide the assessment for these possibilities.

The Level 4 Cyber Security Technologist apprenticeship is highly technical, so whilst employers can select their own entry criteria, they should include; at least 5 GCSEs including English and Mathematics and have achieved a

Level 2 or equivalent qualification as a minimum to help ensure success.

In many cases this type of apprenticeship can demand a higher capability of English and maths than is taught at GCSE or A-Level. For example, advanced report writing, budgeting, complex structured explanations and/or advanced formulae and statistics. The ATP will provide both functional and advanced English and maths diagnostics and teaching to ensure each apprentice is fully supported in these areas.

Programme Duration:

This apprenticeship is delivered over 24 months for full-time employees. For part-time employees the term may be extended depending on the contracted hours.

Delivery Model:

Apprenticeship training is delivered through a blend of weekly live virtual classrooms and regular mentoring sessions that are held on a one-to-one basis.

These live classrooms are held through Microsoft Teams. This software provides the full suite of educational tools including everything you would find in a conventional classroom and more e.g. live open interactions, private breakout rooms, note and question queues and interactive illustration boards. We can also use movie green screen technology for lesson illustrations.

A full timetable for the training, mentoring, exams and assessments is provided at the outset. Progress is reviewed at 12-week intervals in a meeting between the mentor, apprentice and employer (typically the apprentice's line manager).

Employers and apprentices have full visibility of progress in real-time by accessing the e-portfolio system, alternatively regular updates can be provided by other means if preferred.

End Point Assessment (EPA):

Aside from qualifications that can be obtained by doing an apprenticeship, the most important and valuable goal is what has been achieved during the programme.

Successful apprentices will obtain a Pass, Merit or Distinction in their apprenticeship. The way a Pass, Merit or Distinction is determined is at a stage called End Point Assessment which takes place once all the leaning has been completed. Like all examinations, a mock will take place before the final assessment.

Once all components of the apprenticeship have been achieved including the mock, a final review is conducted to ensure everything has been covered, this is called gateway. Then the apprentice will undergo their EPA.

The EPA for this programme consists of:

1. Portfolio of Evidence demonstrating work on 6-8 projects covering all the criteria
2. A project report
3. Knowledge test
4. Scenario demonstration with questioning
5. A structured interview with the assessors exploring the project, portfolio of evidence and employer reference

Programme Structure:

Common/Core Technical Competencies and Skills:

- Identify cyber vulnerabilities to ensure security is maintained
- Identify security threats and hazards, service or processes to inform risk assessments and design of security features
- Research and investigate attack techniques and recommend ways to defend against them
- Support cyber security risk assessments, audits and incident management
- Develop security designs with design justification to meet the defined cyber security parameters
- Configure, deploy and use computer, digital network and cyber security technology
- Develop program code or scripts for a computer or other digital technology for example an industrial control system
- Write reports, give verbal reports and presentations in the context of the cyber security role
- Manage cyber security operations processes in accordance with organisational policies, standards and business requirements
- Participate in cyber war gaming and simulations (technical & non-technical). for example to better understand cyber-attack and defence, rehearse responses, test and evaluate cyber security techniques
- Keep up to date with industry trends and developments to enhance relevant skills, taking responsibility for own professional development

Cyber Security Engineer Pathway:

The Cyber Security Engineer is the most technology focused role in the occupation and will typically design, build and test secure networks or security products or systems with a particular focus on the security aspects of the design.

Typical job titles may include:

- Cyber Security Engineer
- Cyber Security Consultant
- Cyber Security Architect
- Cyber Security Analyst
- Cyber Security Specialist
- IT Security Technician
- Embedded Engineer

Technical Competencies and Skills:

Work from a given design requirement to design, build and test digital networks:

- Networking: OSI and TCP/IP models, data, protocols and how they relate to each other. Main routing protocols; main factors affecting network performance including typical failure modes in protocols and approaches to error control; virtual networking
- Functions and features of at least three Operating Systems (OS) and their security functions and associated security features
- Functions and features of significant digital system components; typical architectures; common vulnerabilities in digital systems; principles and common practice in digital system security
- Programming or scripting languages

Analyse security requirements and develop a security case taking account of all applicable laws and regulations:

- Cyber security concepts. Why cyber security matters to business and society. Security assurance concepts and how assurance may be achieved in practice including penetration testing and extrinsic assurance methods
- Applicability and how to apply the appropriate law, regulations and standards specifically relevant to cyber security. To include laws, regulations & standards relating to personal data and privacy (e.g. Data Protection Act 2018 implementing General Data Protection Regulation), use of digital systems (e.g. Computer Misuse Act 1990); regulatory standards for cyber security, intelligence collection and law enforcement (e.g. Intelligence Services Act 1994, Regulation of Investigatory Powers Act 2000; standards for good practice in cyber security (e.g. ISO 27001, CyberEssentials, NIST) and any updates or additions
- Analysis of employer or customer requirements to derive security objectives and taking account of the threats and overall context, to develop security cases which set out proposed security measures with reasoned justification

Implement structured and reasoned security controls in a digital system in accordance with a security case:

- Common security architectures and methodologies, reputable security architectures that incorporate hardware and software components. Uses cyber security technology components in digital systems to provide security functionality including use of hardware and software to implement security controls
- Basic terminology and concepts of cryptography, common cryptography techniques, effective key management and the main techniques used for legal, regulatory and export issues specific to cryptography
- Security management systems, including governance, organisational structure, roles, policies, standards, guidelines and how these all work together to deliver the identified security outcomes

Prevent security breaches using a variety of tools techniques and processes:

- Main types of common attack techniques, the role of human behaviour, including the significance of the 'insider threat'. How attack techniques combine with motive and opportunity to become a threat. Techniques and strategies to defend against attack techniques and mitigate hazards
- The significance of trends in cyber security threats. Performing risk analysis. How to deal with emerging attack techniques (including 'zero day'), hazards and vulnerabilities relevant to the digital systems and business environment
- Ethical principles and codes of good practice of at least one significant cyber security professional body and the ethical responsibilities of a cyber security professional

Cyber Defend and Respond Pathway:

The Cyber Defender & Responder is more operationally focused, configuring and operating secure systems to prevent security breaches or monitoring systems to detect and respond to security breaches.

Typical job titles may include:

- Cyber Security Analyst
- Cyber Security Operator
- Forensics & Incident Response Analyst
- Cyber Security Administrator
- Information Security Officer
- Secure Operations Centre (SOC) Analyst
- Network Intrusion Analyst
- Incident Response Centre (IRC) Analyst
- Network Operations Centre (NOC) Security Analyst

Technical Competencies and Skills:

Manage local response to non-major cyber security incidents:

- Lifecycle and service management to an established standard at a foundation level, for example Information Technology Infrastructure Library (ITIL) foundation level
- Cyber incident processes, including response, management and evidence collection/preservation requirements to support investigation
- Applicability and how to apply the appropriate law, regulations and standards specifically relevant to cyber security. To include laws, regulations & standards relating to personal data and privacy (e.g. Data Protection Act 2018 implementing General Data Protection Regulation), use of digital systems (e.g. Computer Misuse Act 1990); regulatory standards for cyber security, intelligence collection and law enforcement (e.g. Intelligence Services Act 1994, Regulation of Investigatory Powers Act 2000; standards for good practice in cyber security (e.g. ISO 27001, CyberEssentials, NIST) and any updates or additions
- Analysis of employer or customer requirements to derive security objectives and taking account of the threats and overall context, to develop security cases which set out proposed security measures with reasoned justification
- Ethical principles and codes of good practice of at least one significant cyber security professional body and the ethical responsibilities of a cyber security professional

Monitor technology systems (for example computer networks and computer systems) in real time to detect cyber security incidents, breaches and intrusions:

- Main types of common attack techniques, the role of human behaviour, including the significance of the 'insider threat'. How attack techniques combine with motive and opportunity to become a threat. Techniques and strategies to defend against attack techniques and mitigate hazards
- The significance of trends in cyber security threats. Performing risk analysis. How to deal with emerging attack techniques (including 'zero day'), hazards and vulnerabilities relevant to the digital systems and business environment

Integrate and correlate information from a variety of sources and form an informed judgement on whether an indicator constitutes a likely security incident, breach or intrusion:

- Cyber security concepts. Why cyber security matters to business and society. Security assurance concepts and how assurance may be achieved in practice including penetration testing and extrinsic assurance methods

Respond to a suspected security incident, breach or intrusion in accordance with organisation procedures any defined service level agreements or performance targets:

- Knowledge taught is taken from the competency criteria set out above applied to this context

Prevent security breaches using a variety of tools techniques and processes:

- Networking: OSI and TCP/IP models, data, protocols and how they relate to each other. Main routing protocols; main factors affecting network performance including typical failure modes in protocols and approaches to error control; virtual networking
- Functions and features of at least three Operating Systems (OS) and their security functions and associated security features
- Functions and features of significant digital system components; typical architectures; common vulnerabilities in digital systems; principles and common practice in digital system security
- Programming or scripting languages

Cyber Risk Analyst Pathway:

The Cyber Risk Analyst Focuses on risk assessment, analysis and giving advice on risk mitigations. The roles may support formal security governance, regulatory & compliance (GRC).

Typical job titles may include:

- Cyber Risk Analyst
- Governance and Compliance Analyst
- Cyber Intelligence Researcher

Technical Competencies and Skills:

Analyse security requirements and develop a security case taking account of all applicable laws and regulations

- Cyber security concepts. Why cyber security matters to business and society. Security assurance concepts and how assurance may be achieved in practice including penetration testing and extrinsic assurance methods
- Applicability and how to apply the appropriate law, regulations and standards specifically relevant to cyber security. To include laws, regulations & standards relating to personal data and privacy (e.g. Data Protection Act 2018 implementing General Data Protection Regulation), use of digital systems (e.g. Computer Misuse Act 1990); regulatory standards for cyber security, intelligence collection and law enforcement (e.g. Intelligence Services Act 1994, Regulation of Investigatory Powers Act 2000; standards for good practice in cyber security (e.g. ISO 27001, CyberEssentials, NIST) and any updates or additions
- Analysis of employer or customer requirements to derive security objectives and taking account of the threats and overall context, to develop security cases which set out proposed security measures with reasoned justification

Conduct cyber security risk assessments and audits

- Networking: OSI and TCP/IP models, data, protocols and how they relate to each other. Main routing protocols; main factors affecting network performance including typical failure modes in protocols and approaches to error control; virtual networking
- Functions and features of at least three Operating Systems (OS) and their security functions and associated security features
- Main types of common attack techniques, the role of human behaviour, including the significance of the 'insider threat'. How attack techniques combine with motive and opportunity to become a threat. Techniques and strategies to defend against attack techniques and mitigate hazards
- The significance of trends in cyber security threats. Performing risk analysis. How to deal with emerging attack techniques (including 'zero day'), hazards and vulnerabilities relevant to the digital systems and business environment
- Functions and features of significant digital system components; typical architectures; common vulnerabilities in digital systems; principles and common practice in digital system security
- Programming or scripting languages
- Ethical principles and codes of good practice of at least one significant cyber security professional body and the ethical responsibilities of a cyber security professional
- Risk assessment and audit methodologies/ approaches to risk treatment. Uses approaches to identifying vulnerabilities in organisations and security management systems and threat intelligence lifecycle. Understands the role of the risk owner in contrast with other stakeholders

Develop information security policies to achieve security outcomes within a defined scope

Security management systems, including governance, organisational structure, roles, policies, standards, guidelines and how these all work together to deliver the identified security outcomes

Design and implement security awareness campaigns

- Knowledge taught is taken from the competency criteria set out above applied to this context

Behavioural Development Embedded:

- Logical - Applies logical thinking, for example, uses clear and valid reasoning when making decisions related to undertaking the work instructions
- Analytical - working with data effectively to see patterns, trends and draw meaningful conclusions
- Works independently and takes responsibility. For example works diligently regardless of how much they are being supervised, and stays motivated and committed when facing challenges
- Shows initiative, being resourceful when faced with a problem and taking responsibility for solving problems within their own remit
- Thorough & organised. For example uses their time effectively to complete work to schedule and takes responsibility for managing their own work load and time
- Works effectively with a wide range of people in different roles, internally and externally, with a regard to inclusion & diversity policy
- Communicates effectively in a wide variety of situations for example contributing effectively to meetings and presenting complex information to technical and non-technical audiences
- Maintains a productive, professional and secure working environment
- Creative - taking a variety of perspectives, taking account of unpredictable adversary and threat behaviours and approaches, bring novel and unexpected solutions to address cyber security challenges
- Problem Solving - Identifies issues quickly, solves complex problems and applies appropriate solutions. Dedicated to finding the true root cause of any problem and find solutions that prevent recurrence

The designated mentor 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.

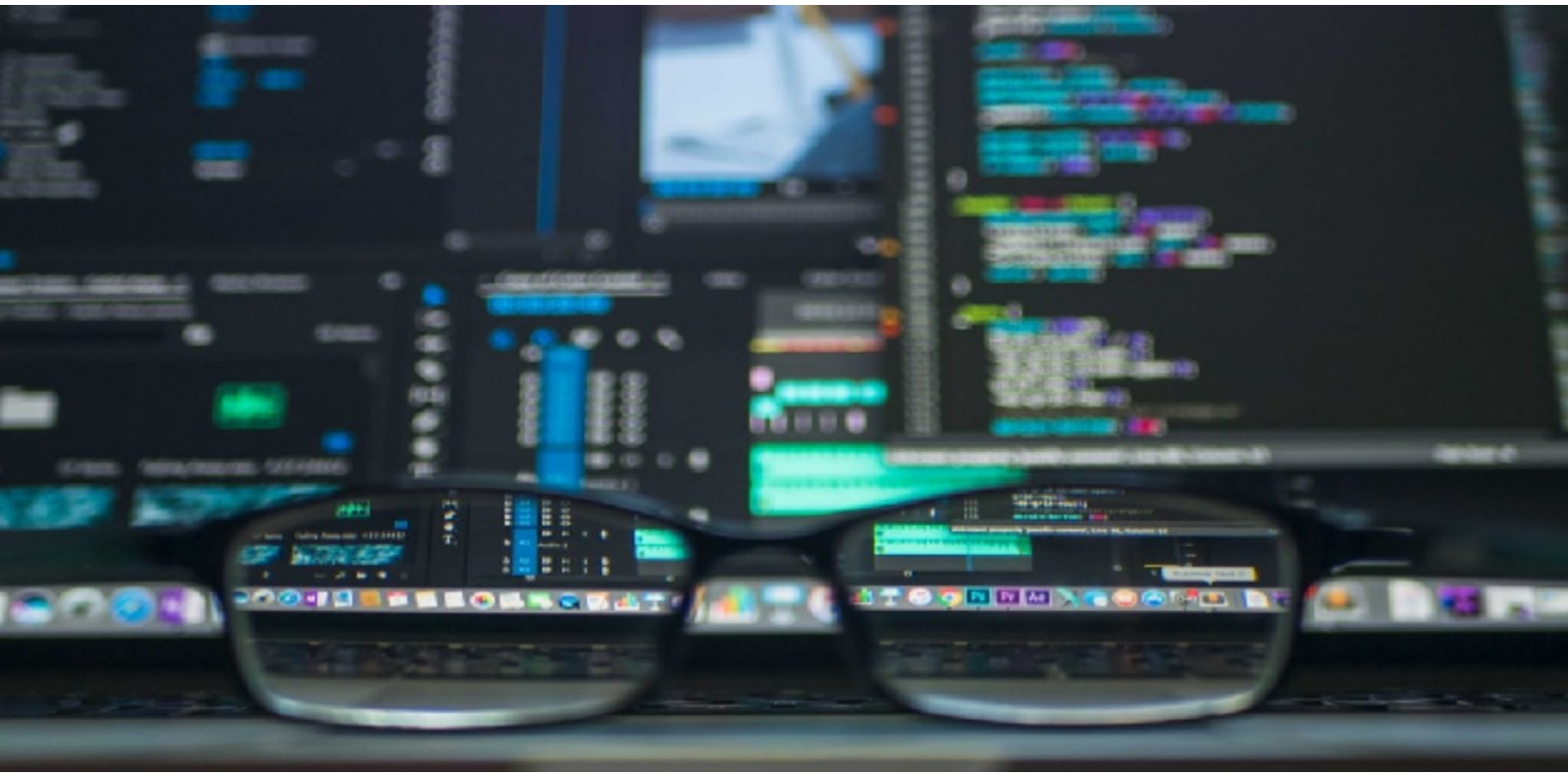
Progression:

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:

To configure an ideal apprenticeship we will meet with you, discuss your needs, present the options and collaborate to determine the best apprenticeships to meet your needs. We will provide ongoing support including:

- Recruitment of candidates
- Quality assured Information Advice and Guidance
- Updates and information on legislation and funding
- Support and guidance for apprentice and employer throughout the apprenticeship
- Access to a comprehensive suite of resources and support material via OneFile
- Industry specialist qualified trainers and mentors



If you have any questions about this apprenticeship Standard or would like to book an information session, please contact our team T. 0330 380 0249 or E. info@theatp.co.uk