# National Apprenticeship - Occupational Profile

| | |
|---|---|
| Apprenticeship Title | Cybersecurity |
| NFQ Level | 6 |
| Duration | 2 Years |
| Typical tasks/ responsibilities | The Cybersecurity worker applies an understanding of cyber threats, hazards, risks, controls, measures and mitigations to protect organisations, systems and people.<br>Those focused on the technical side, work in areas such as security design and architecture, security testing, investigations & response.<br>Those focused on the risk analysis side, concentrate on areas such as operations, risk, governance & compliance.<br>Specialists 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 organisations requirements. |

**On successful completion of the proposed apprenticeship, a Cybersecurity expert will be able to:**

## Knowledge

- Understand why cybersecurity matters - the importance to business and society
- Understand basic data security 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
- Understand security assurance concepts (i.e. can explain what “assurance” means in security terms, and difference between ‘trustworthy’ and ‘trusted’) and how assurance may be achieved in practice (i.e. can explain what penetration testing is and how it contributes to assurance; and extrinsic assurance methods)
- Understand how to build a security case - deriving security objectives with reasoned justification in a representative business scenario
- Understand cybersecurity concepts applied to ICT infrastructure - can describe the fundamental building blocks and typical architectures and identify common vulnerabilities in networks and systems
- Understand attack techniques and sources of threat - can describe the main types of common attack techniques and the role of human behaviour. Explains how attack techniques combine with motive and opportunity to become a threat
- Understand cyber defence - describes ways to defend against attack techniques

**Knowledge**
(cont'd).

- Understand relevant laws and ethics - describes security standards, regulations and their consequences across at least two sectors; the role of criminal and other law; key relevant - features of Irish and international law
- Understand the existing threat landscape - can describe and know how to apply relevant techniques for horizon scanning including use of recognised sources of threat intelligence
- Understand threat trends - can describe the significance of identified trends in cybersecurity and understand the values and risks of this analysis

**Skills**

- Discover (through a mix of research and practical exploration) vulnerabilities in a system
- Analyse and evaluate security threats and hazards to a system, service or process. Is aware of, and demonstrates use of relevant external sources of threat intelligence or advice. Combines different sources to create an enriched view
- Research and investigate common attack techniques and recommends how to defend against them. Is aware of, and demonstrates use of relevant external sources of vulnerabilities (e.g. OWASP)
- Undertake a security risk assessment for a system without direct supervision and propose remediation advice in the context of the employer
- 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 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)
- Identify and follow organisational policies and standards for information and cybersecurity
- Operate according to service level agreements or employer-defined performance targets
- 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

### Competencies

- Exhibit logical and creative thinking
- Exhibit analytical and problem solving ability
- Work autonomously and within teams
- Use own initiative
- Exhibit a thorough and organised approach to working practice
- Work with a range of internal and external people
- Communicate effectively in a variety of situations
- Maintain productive, professional and secure working environment

### Industry/industries served by the apprenticeship

- Telecoms/technology
- Government
- Finance
- Business support
- Manufacturing
- Education
- Utilities
- Health & pharma
- Information and communication (ICT)
- Financial and insurance activities
- Manufacturing
- Human health & welfare
- Public administration and defence
- Wholesale and retail trade
- Education
- Professional, scientific and technical activities
- Accommodation and food service activities
- Arts, entertainment and recreation
- Agriculture, forestry and fishing
- Utilities
- Construction
- Transportation and storage
- Administrative and support

**Proposed minimum entry requirements for apprentices on the programme**

- Must be 18 years or older
- Must have achieved a passing grade in 5 or more subjects (to include Maths and English) at Ordinary Level in the Leaving Certificate. For those who may not hold some or all of these certifications, eligibility for entry will be decided through the Recognition of Prior Learning
- Must complete suitability tests (aptitude and knowledge)