Cyber Security Technician Apprenticeship

EMPLOYER FACTSHEET

GROW YOUR OWN TALENT

Monitor for security threats, install and maintain security measures like firewalls, antivirus software and respond to security incidents.

Key Information

Level	3
Duration	18 months
Entry requirements	- 16 years or over. - Please contact our Apprenticeship team for further entry requirements.
Delivery	A minimum of 30 hours of on-the-job training at workplace per week and 1 day learning. HRUC offer remote and face to face delivery.
Occupation summary	A Level 3 Cyber Security Technician provides fundamental support within a security team, implementing defined security controls, monitoring events, and responding to common threats like phishing and malware. Key duties include configuring firewalls, deploying anti-virus software, applying security updates, assessing vulnerabilities, and managing access rights, all under supervision.
Typical future roles	Incident response technician, Cyber security administrator, Information security analyst, Penetration tester, Security analyst, Security operations analyst, Threat and risk analyst.
Professional Recognition	This standard aligns with the following professional recognition: • UK Cyber Security Council for Associate • BCS, The Chartered Institute for IT for Associate BCS membership (AMBCS) and Professional • Registration for IT Technicians (RITTech) for Level 3 • Chartered Institute for Information Security for Accredited Affiliate.

Choose a Trusted Provider

We are a top provider in London with consistently high success rates

We are the largest college provider of apprenticeships in west London

We work with major companies including Brunel University London, Martin-Baker Aircraft Limited & Menzies etc.

Government funding may be available. Eligibility and criteria apply

Employers involved in creating this standard:

Babcock International Group, BAE Systems, Bromford Housing Association, Cavendish Nuclear, First Group, MVV, Ministry of Defence, Pendennis Shipyard, Royal Navy, RWE Energy, Rolls Royce.

01895 853780
employers@hruc.ac.uk
www.hruc.ac.uk/employers
@HRUCSkills

HRUC

Apprenticeships & Skills

Harrow, Richmond & Uxbridge Colleges

Role Profile

A Level 3 Cyber Security Technician provides fundamental support within a security team, implementing defined security controls, monitoring events, and responding to common threats like phishing and malware.

Key duties include configuring firewalls, deploying anti-virus software, applying security updates, assessing vulnerabilities, and managing access rights, all under supervision. They also play a role in maintaining security inventories, gathering threat intelligence, documenting security events, and working with other teams to ensure compliance with policies and procedures.

The key responsibilities of a Cyber Security Technician include monitoring and assessing security events, performing vulnerability assessments, managing access rights, documenting security issues, and maintaining technical security controls. They also assist with information security training, conduct risk assessments, and produce information management reports to communicate findings to stakeholders.

English & Maths

Apprentices without level 2 English and maths will need to achieve these prior to the Apprenticeship Assessment. For those with an education, health and care plan or a legacy statement the apprenticeships English and maths minimum requirement is Entry Level 3 and British Sign Language qualification are an alternative to English qualifications for whom this is their primary language.

Modules and Content Summary

Knowledge

K1: Principles of organisational information security governance and the components of an organisation's cyber security technical infrastructure including hardware, operating systems, networks, software and cloud

K2: Cyber security policies and standards based on an Information Security Management System (ISMS)

K3: Types of physical, procedural and technical controls

K4: Awareness of how current legislation relates to or impacts upon the occupation including Data Protection Act, Regulation of Investigatory Powers Act, Human Rights Act, Computer Misuse Act, Freedom of Information Act, Official Secrets Act, Payment Card Industry Data Security Standard (PCI-DSS), Wireless and Telegraphy Act, professional body codes of conduct, ethical use of information assets

K5: Cyber security awareness and components of an effective security culture, different organisational structures and cultures, the importance of maintaining privacy and confidentiality of an organisation's information and the impact of a poor security culture

K6: Principles of cyber security compliance and compliance monitoring techniques

K7: Core terminology of cyber security – confidentiality, integrity, availability (the CIA triad), assurance, authenticity, identification, authentication, authorization, accountability, reliability, non-repudiation, access control

K8: Common security administrative operational tasks e.g. patching, software updates, access control, configuring a range of firewalls, security incident and event management tools (SIEM) and protection tools (Anti-virus, Anti-malware, Anti-spam)

K9: Cryptography, certificates and use of certificate management tools

K10: Processes for detecting, reporting, assessing, responding to, dealing with and learning from information security events

K11: Principles of identity and access management - authentication, authorisation and federation - and the inter-relationship between privacy and access rights and access control, and the types of access control, access control mechanisms and application control

K12: Types of digital information assets used in a controlled environment and the need to maintain an inventory of information assets used in a controlled environment and the need for and practice of secure information asset disposal

K13: Disaster prevention and recovery methods and the need for continuity of service planning and how an organisation might implement basic disaster prevention and recovery practices using conventional and incremental secure backup and recovery techniques and tools both onsite and offsite including geographic considerations

K14: Categories of cyber security vulnerabilities and common vulnerability exposures –software misconfiguration, sensitive data exposure, injection vulnerabilities, using components with known vulnerabilities, insufficient logging and monitoring, broken access control and authentication, security misconfiguration, incorrect cross-site validation.

Knowledge

K15: Components of a vulnerability assessment scope and techniques to evaluate the results of a vulnerability assessment and provide recommendations based upon the evidence provided by the vulnerability assessment tools. The impact that vulnerabilities might have on an organisation and common vulnerability assessment tools and their strengths and weaknesses

K16: Threat sources and threat identification and network reconnaissance techniques and the impact that threats might have on an organisation

K17: Types of information security events – brute force attack, malware activity, suspicious user behaviour, suspicious device behaviour, unauthorized system changes

K18: Computer forensic principles – the importance of ensuring that evidence is not contaminated and maintaining the continuity of evidence without compromising it

K19: Standard information security event incident, exception and management reporting requirements and how to document incident and event information as part of a chain or evidence

K20: Common information security policies – acceptable use, incident management, patching, anti-virus, BYOD, access control, social media, password, data handling and data classification, IT asset disposal

K21: Cyber security audit requirements, procedures and plans, need to obtain and document evidence in an appropriate form for an internal or external auditor to review

K22: The significance of customer issues, problems, business value, brand awareness, cultural awareness/ diversity, accessibility, internal/ external audience, level of technical knowledge and profile in a business context

K23: Evolving cyber security issues in the digital world including the application to critical national infrastructure, communications technologies, the need for information assurance and governance, control systems and internet of things (IoT) devices

K24: Different learning techniques and the breadth and sources of knowledge and sources of verified information and data

K25: Importance of maintaining privacy and confidentiality of an organisations information and the impact of a poor security culture

K26: Concepts of service desk delivery and how to respond to requests for assistance received by a service desk and be able to describe different methods of escalation, when to escalate to a higher level where necessary and the need to communicate accurately and appropriately during an escalation

K27: Risk assessment, risk management and business impact analysis principles

K28: How their occupation fits into the wider digital landscape and any current or future regulatory requirements

K29: How to use data ethically and the implications for wider society, with respect to the use of data

K30: Roles within a multidisciplinary team and the interfaces with other areas of an organisation.

Behaviour

B1: Manage own time to meet deadlines and manage stakeholder expectations

B2: Work independently and take responsibility for own actions within the occupation

B3: Use own initiative

B4: A structured approach to the prioritisation of tasks

B5: Treat colleagues and external stakeholders fairly and with respect without bias or discrimination

B6: Act in accordance with occupation specific laws, regulations and professional standards and not accept instruction that is incompatible with any of these

B7: Review own development needs in order to keep up to date with evolution in technologies, trends and innovation using a range of sources.

Skills

S1: Follow information security procedures

S2: Maintain information security controls

S3: Develop information security training and awareness resources

S4: Monitor the effectiveness of information security training and awareness

S5: Handle and assess the validity of security requests from a range of internal and external stakeholders

S6: Follow technical procedures to install and maintain technical security controls

S7: Monitor and report information security events

S8: Recognise when and how to escalate information security events in accordance with relevant procedures and standards

S9: Review and modify access rights to digital information systems, services, devices or data

S10: Maintain an inventory of digital information systems, services, devices and data storage

S11: Scopes cyber security vulnerability assessments

S12: Evaluate the results of a cyber security vulnerability assessment

S13: Perform routine threat intelligence gathering tasks through consulting external sources

S14: Undertake digital information risk assessments

S15: Identify and categorise threats, vulnerabilities and risks in preparation for response or escalation

S16: Document cyber security event information whilst preserving evidence

S17: Draft information management reports using standard formats appropriate to the recipients

S18: Review and comment upon cyber security policies, procedures, standards and guidelines

S19: Perform cyber security compliance checks

S20: Translate audit requirements and collate relevant information from log files, incident reports and other data sources

S21: Communication skills to co-operate as part of a multi-functional, multi-disciplinary team using a range of technical and non-technical language to provide an effective interface between internal or external users and suppliers

S22: Keep up to date with legislation and industry standards related to the implementation of cyber security in an organisation.

Assessment

To complete the Cyber Security Apprenticeship, apprentices will be expected to complete an Apprenticeship Assessment which will include 3 components:

- Observation / Practical Assessment
- Interview or panel discussion
- Written or online knowledge test.

01895 853780
employers@hruc.ac.uk
www.hruc.ac.uk/employers
@HRUCSkills

HRUC
Apprenticeships & Skills
Harrow, Richmond & Uxbridge Colleges