Institute for Apprenticeships
& Technical Education

CYBER SECURITY TECHNOLOGIST (2021)

Details of standard

This standard has options. Display duties and KSBs for:

All

Occupation summary

This occupation is found in all sectors and organisations that employ technology, for example Digital, Telecoms, Technology, Business Services, Defence, Government, Finance, Health, Retail, Critical National Infrastructure, Transport, Automotive sectors; and in all types and sizes of organisation including large corporates, public sector bodies, academic institutions, charities, and small and medium enterprise (SME).

The broad purpose of the occupation is to apply an understanding of cyber security to protect organisations, systems, information, personal data and people from attacks and unauthorised access.

Fighting cyber security threats is a multi-billion-pound industry, and one that continues to grow as threats from the likes of malware, ransomware, phishing, DDoS attacks and hacking increase. Organisations both large and small are turning to cyber security professionals to help them keep their commercial and financial data, websites, infrastructure sites and their customers' details safe.

With almost all personal data now stored online, cyber security attacks have the potential to completely ruin businesses - not to mention people's lives - in the process. There are often

news stories about high-profile attacks, such as those on the NHS, Yahoo and LinkedIn, meaning that organisations are becoming increasingly concerned with any potential leaks that could occur. In fact, nearly half of all UK businesses experienced some form of attack in the last 12 months. As a cyber-security technologist, you will be part of the response to those attacks.

Cyber Security Technologists all require an understanding of security concepts and technology and how to mitigate risks arising from threats. The specific tasks undertaken vary depending on what needs to be achieved by the team at any particular time. Some tasks may be very technical, others may be more analytical, business or user focused. All roles in this occupation work to achieve required cyber 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 requirement.

The Cyber Security Technologist standard has three distinct options. At the end of the apprenticeship you will be competent in either:

1) 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 include: Cyber Security Engineer, Cyber Security Consultant, Cyber Security Architect, Cyber Security Analyst, Cyber Security Specialist, IT Security Technician, Embedded Engineer.

2) 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 include: Cyber Security Consultant, Cyber Security Analyst, Cyber Risk Analyst, Intelligence Researcher, Cyber Security Specialist, Information Security Analyst, Governance & Compliance Analyst, Information Security Assurance & Threat Analyst, Information Security Auditor.

3) 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 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.

In their daily work, an employee in this occupation interacts with a broad range of people from their own organisation and externally including suppliers and customers, technical specialists, non-specialists, peers and senior representatives. The roles are typically office or computer room/lab based. Some employers will also have security clearance requirements, which may impose residency or nationality restrictions. An employee in this occupation will be responsible for their own work, work as part of a team including different levels of technical and non-technical skills, and may also be required to supervise work, budgets and other staff.

Typical job titles include:

Cyber operations manager | Cyber risk analyst | Intelligence researcher | Security analyst | Security architect

Core occupation duties

DUTY	KSBS
Duty 1 Identify cyber vulnerabilities in a system to ensure security is maintained.	K1 K2 K3 K4 K5 K11 K12 K13 K15 K16 K17 S1 S9 B1 B2 B4 B5 B6 B7 B8 B9
Duty 2 Identify security threats and hazards to a system, service or processes to inform risk assessments and design of security features	K4 K5 K11 S2 S9 S17 B1 B2 B5 B6 B7 B9 B10
Duty 3 Research and investigate attack techniques and recommend ways to defend against them	K2 K4 K5 K13 K15 S3 S9 B1 B2 B3 B4 B5 B6 B7 B8 B9 B10
Duty 4 Support cyber security risk assessments, cyber security audits and cyber security incident management	K4 K5 K7 K8 K9 K14 S4 B1 B2 B3 B5 B6 B7 B8 B10
Duty 5 Develop security designs with design justification to meet the defined cyber security parameters.	K3 K4 K8 K10 S5 S6 B1 B2 B9 B10
Duty 6 Configure, deploy and use computer, digital network and cyber security technology.	K1 K2 K16 K17 S8 B1 B3 B4 B10
Duty 7 Develop program code or scripts for a computer or other digital technology for example an industrial control system	K1 K16 K17 S13 B1 B2 B3 B5 B8 B10
Duty 8 Write reports, give verbal reports and presentations in the context of the cyber security role	S27

	B1 B3 B4 B5 B7 B9
Duty 9 Manage cyber security operations processes in accordance with organisational policies and standards and business requirements.	K3 K6 K8 K9 K15 S7 B1 B3 B5 B6 B8
Duty 10 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	K1 K2 K4 K9 K15 K16 K17 S1 S2 S4 B1 B2 B3 B4 B5 B6 B7 B8 B9 B10
Duty 11 Keep up to date with industry trends and developments to enhance relevant skills and take responsibility for own professional development	K8 K9 B3

Option duties

Cyber Security Engineer duties

DUTY	KSBS
Duty 12 Work from a given design requirement to design, build and test digital networks	K1 K2 K16 K17 S10 B1 B3 B5 B8 B10
Duty 13 Analyse security requirements and develop a security case taking account of all applicable laws and regulations.	K3 K8 K10 S5 B1 B2 B3 B5 B8 B9 B10
Duty 14 Implement structured and reasoned security controls in a digital system in accordance with a security case	K12 K13 K15 S11 S12 S14 B1 B2 B3 B4 B5 B6 B7 B8 B9 B10
Duty 22 Prevent security breaches using a variety of tools techniques and processes.	K1 K2 K3 K4 K5 K8 K9 K15 K16 K17 S1 S2 S3 S15 S28 B1 B2 B3 B4 B5 B6 B7 B8 B9 B10

Cyber Risk Analyst duties

DUTY	KSBS
Duty 13 Analyse security requirements and develop a security case taking account of all applicable laws and regulations.	K3 K8 K10 S5 B1 B2 B3 B5 B8 B9 B10
Duty 15 Conduct cyber security risk assessments	K1 K2 K3 K4 K5 K8 K14 K16 K17 S1 S2 S3 S4 S16 S17 S22 B1 B2 B3 B4 B5 B6 B7 B8 B9 B10
Duty 16 Conduct cyber security audits	K8 K9 K14 S20 B1 B3 B5 B6 B7 B8
Duty 21 Develop information security policies to achieve security outcomes within a defined scope	K3 K8 K15 S18 S19 B1 B2 B3 B4 B5 B6 B7 B8 B9 B10
Duty 23 Design and implement security awareness campaigns	K3 K4 K8 S17 S23 S24 B3 B4 B5 B6 B7 B9

Cyber Defend & Respond duties

DUTY	KSBS
Duty 17 Manage local response to non-major cyber security incidents	K6 K7 K8 K9 K15 S21 S30 B1 B2 B3 B4 B5 B6 B7 B8 B10
Duty 18 Monitor technology systems (for example computer networks and computer systems) in real time to detect cyber security incidents, breaches and intrusions	K4 K5 K6 K7 K8 S2 S7 S25 B1 B2 B3 B4 B5 B6 B7 B8
Duty 19 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.	K3 K4 K5 S26 S27 S29 B1 B2 B3 B4 B5 B6 B7 B8 B10
Duty 20 Respond to a suspected security incident, breach or intrusion in accordance with organisation procedures any defined service level agreements or performance targets.	K6 K7 K9 K15 S7 B1 B5 B6 B7 B8
Duty 22 Prevent security breaches using a variety of tools techniques and processes.	K1 K2 K3 K4 K5 K8 K9 K15 K16 K17 S1 S2 S3 S15 S28 B1 B2 B3 B4 B5 B6 B7 B8 B9 B10

KSBs

Knowledge

K1: Principles of networks: OSI and TCP/IP models, 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; virtual networking

K2: the concepts, main functions and features of at least three Operating Systems (OS) and their security functions and associated security features.

K3: Cyber security concepts and 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.

K4: the main types of common attack techniques; also the role of human behaviour, including the significance of the 'insider threat'. Including: how attack techniques combine with motive and opportunity to become a threat. Techniques and strategies to defend against attack techniques and mitigate hazards

K5: the significance of identified trends in cyber security threats and understand the value and risk of this analysis. How to deal with emerging attack techniques (including 'zero day'), hazards and vulnerabilities relevant to the digital systems and business environment.

K6: lifecycle and service management practices to an established standard to a foundation level for example Information Technology Infrastructure Library (ITIL) foundation level.

K7: cyber incident response processes, incident management processes and evidence collection/preservation requirements to support incident investigation

K8: Understands the main features, applicability and how to apply the significant law, regulations and standards relevant specifically 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

K9: 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.

K10: how to analyse employer or customer requirements to derive security objectives and taking account of the threats and overall context develop a security case which sets out the proposed security measures in the context with reasoned justification

K11: horizon scanning including use of recognised sources of threat intelligence and vulnerabilities.

K12: common security architectures and methodologies; be aware of reputable security architectures that incorporates hardware and software components, and sources of architecture patterns and guidance. How cyber security technology components are typically deployed in digital systems to provide security functionality including: hardware and software to implement security controls

K13: the basic terminology and concepts of cryptography; common cryptography techniques in use; the importance of effective key management and the main techniques used; legal, regulatory and export issues specific to the use of cryptography

K14: risk assessment and audit methodologies and approaches to risk treatment; approaches to identifying the vulnerabilities in organisations and security management systems; the threat intelligence lifecycle; the role of the risk owner in contrast with other stakeholders

K15: principles of security management systems, including governance, organisational structure, roles, policies, standards, guidelines and how these all work together to deliver the identified security outcomes.

K16: function and features of significant digital system components; typical architectures; common vulnerabilities in digital systems; principles and common practice in digital system security

K17: programming or scripting languages

Skills

S1: Discover vulnerabilities in a system by using a mix of research and practical exploration

S2: Analyse and evaluate security threats and hazards to a system or service or processes. Use relevant external source of threat intelligence or advice (e.g. National Cyber Security Centre) Combine different sources to create an enriched view of cyber threats and hazards

S3: Research and investigate common attack techniques and relate these to normal and observed digital system behaviour and recommend how to defend against them. Interpret and demonstrate use of external source of vulnerabilities (e.g. OWASP, intelligence sharing initiatives, open source)

S4: Undertake security risk assessments for simple systems without direct supervision and propose basic remediation advice in the context of the employer.

S5: Source and analyse security cases and describe what threats, vulnerability or risks are mitigated and identify any residual areas of concern.

S6: Analyse employer or customer requirements to derive security objectives and taking account of the threats and overall context develop a security case which sets out the proposed security measures in the context with reasoned justification

S7: Identify and follow organisational policies and standards for information and cyber security and operate according to service level agreements or other defined performance targets.

S8: Configure, deploy and use computer, digital network and cyber security technology.

S9: Recommend improvements to the cyber security posture of an employer or customer based on research into future potential cyber threats and considering threat trends.

S10: Design, build, test and troubleshoot a network incorporating more than one subnet with static and dynamic routes, to a given design requirement without supervision. Provide evidence that the system meets the design requirement.

S11: Analyse security requirements given (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.) for a given system or product. Identify conflicting requirements and propose, with reasoning, resolution through appropriate trade-offs.

S12: Design and build, systems in accordance with a security case within broad but generally well-defined parameters. This should include selection and configuration of typical security hardware and software components. Provide evidence that the system has properly implemented the security controls required by the security case

S13: Write program code or scripts to meet a given design requirement in accordance with employers' coding standards

S14: Design systems employing encryption to meet defined security objectives. Develop and implement a plan for managing the associated encryption keys for the given scenario or system.

S15: Use tools, techniques and processes to actively prevent breaches to digital system security.

S16: Conduct cyber-risk assessments against an externally (market) recognised cyber security standard using a recognised risk assessment methodology.

S17: Identify cyber security threats relevant to a defined context

S18: Develop information security policies or processes to address a set of identified risks, for example from security audit recommendations.

S19: Develop information security policies within a defined scope to take account of legislation and regulation relevant to cyber security.

S20: Take an active part in a security audits against recognised cyber security standards, undertake gap analysis and make recommendations for remediation..

S21: Develop plans for incident response for approval within defined governance arrangements for incident response.

S22: Develop plans for local business continuity for approval within defined governance arrangements for business continuity.

S23: Assess security culture using a recognised approach.

S24: Design and implement a simple ‘security awareness’ campaign to address a specific aspect of a security culture.

S25: Integrate and correlate information from various sources (including log files from different sources, digital system monitoring tools, Secure Information and Event Management (SIEM) tools, access control systems, physical security systems) and compare to known threat and vulnerability data to form a judgement based on evidence with reasoning that the anomaly represents a digital system security breach

S26: Recognise anomalies in observed digital system data structures (including by inspection of network packet data structures) and digital system 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.

S27: Accurately, objectively and concisely record and report the appropriate cyber security information, including in written reports within a structure or template provided.

S28: Configure digital system monitoring and analysis tools (e.g. SIEM tools), taking account of threat & vulnerability intelligence, indicators of compromise.

S29: Undertake root cause analysis of events and make recommendations to reduce false positives and false negatives.

S30: Manage local response to non-major incidents in accordance with a defined procedure.

Behaviours

B1: Logical - Applies logical thinking, for example, uses clear and valid reasoning when making decisions related to undertaking the work instructions

B2: Analytical - working with data effectively to see patterns, trends and draw meaningful conclusions.

B3: 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

B4: Shows initiative, being resourceful when faced with a problem and taking responsibility for solving problems within their own remit

B5: Thorough & organised. For example uses their time effectively to complete work to schedule and takes responsibility for managing their own work load and time

B6: Works effectively with a wide range of people in different roles, internally and externally, with a regard to inclusion & diversity policy

B7: Communicates effectively in a wide variety of situations for example contributing effectively to meetings and presenting complex information to technical and non-technical audiences

B8: Maintains a productive, professional and secure working environment.

B9: 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

B10: 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.

Qualifications

English and Maths

Apprentices without level 2 English and maths will need to achieve this level prior to taking the End-Point Assessment. For those with an education, health and care plan or a legacy statement, the apprenticeship’s English and maths minimum requirement is Entry Level 3. A British Sign Language (BSL) qualification is an alternative to the English qualification for those whose primary language is BSL.

Professional recognition

This standard aligns with the following professional recognition:

- RITTech for level 4

Additional details

Occupational Level:

4

Duration (months):

24

Review

This apprenticeship standard will be reviewed after three years

Version log

VERSION	CHANGE DETAIL	EARLIEST START DATE	LATEST START DATE	LATEST END DATE
1.0	Approved for delivery	04/05/2021	Not set	Not set

Is this page useful?

Yes No

Report a problem with this page