BSc (Hons) Cyber Security Technical Professional

About this course

Course overview

This programme is delivered in partnership by QA and Northumbria University with the degree awarded by Northumbria University.

https://www.youtube.com/watch?v=KHRk3rML67Y

For learners applying to begin their programme in January: QA has two primary objectives during this rapidly evolving period regarding Coronavirus (Covid-19). The first is to ensure the welfare of our learners and staff, and the second is to ensure continuity and access to learning. In line with the sector as a whole and its response to Covid-19, if necessary, we will implement online teaching for this programme to allow you to begin your programme this January.

Funded by Education & Skills Funding Agency

European Union
European Social Fund

PLEASE NOTE: To be eligible for one of our Degree Apprenticeship programmes, learners must:
(1) be **currently in full-time employment** and based in the UK
(2) be interested in completing a Degree Apprenticeship with their **current employer**

The BSc (Hons) Cyber Security Technical Professional Degree Apprenticeship programme is designed to enhance and accelerate career prospects through engaging in a work based learning programme providing opportunities to develop an understanding of cyber security issues and technology solutions and capitalise on opportunities for applied learning within the context of employment. The programme will specifically enable you to develop, update, extend and deepen your knowledge and technical competencies; underpinning professional skills and behaviours to excel as a thorough cyber security professional working in wider business or technology/engineering functions.

To support your development of the qualities listed above, the programme takes a work-related approach in which you will develop knowledge and understanding, your personal capability and be able to apply technical competencies, professional skills and behaviours in cyber security and wider business or a technology/engineering role within your current organisational setting.

Your learning, personal and professional development will therefore be facilitated through a structured research-rich learning programme and supported by a range of learning, classroom and work based learning experiences. This will enable you to embark on a learning programme designed to enhance your future employability and equip you for a career leading or working within a cyber security, technology, engineering and wider business environment.

How will I be taught?

As an apprentice, you are entitled to 20% of your working time off for studying. This will be agreed between your employer, you and us – we can advise how best to do this.

This programme fully utilises blended learning through a range of digital learning resources and teaching that will support you in your studies and work-based learning.

On top of this, you will have day block workshops at your study location to help you contextualise your learning. These are delivered as follows:

- Level 4 – Two 2-day block workshops (6 hours per day) per module

- Level 5 – One 2-day and one 1-day block workshop (6 hours per day) per module
- Level 6 – Two 1-day workshops (6 hours per day) per module

You will also receive regular contact and support from your coach throughout the programme. This can take the form of both face-to-face and virtual contact.

The main method of assessment used is individual coursework and each assessment is designed to enable you to demonstrate module learning outcomes, which in turn support the overall achievement of the learning outcomes of the programme as a whole. A range of coursework approaches will be used throughout the programme. This will include technical projects for technical modules and research-informed assignments for other modules to enable you to develop a sound knowledge base in key areas of cyber security and research-informed work-based projects for “Professional Practice” modules.

Download Programme Handout

Careers

You will be equipped to work in a range of Computing, IT, and Digital Technology roles. These include Cyber Risk Manager; Cyber Risk Analyst; Cyber Research Analyst; Cyber Incident Manager; Cyber Security Engineer; Cyber Security Design Engineer.

If you intend to pursue a masters programme in the future, this programme is an ideal grounding. The technical knowledge, research and study skills that you will acquired provide an excellent foundation for a number of generalist and specialist masters programmes in computing and computing related technologies.

Modules

All modules are core and worth 20 credits unless otherwise stated.

Level 4

Computer Systems and Digital Logic

In this module you will develop knowledge and skills in Computer architecture, digital logic, machine level representation of data and in testing and how to debug programs in low level language. You will subsequently be able to apply this knowledge and skill in your own context, and apply this to solve problems and recommend potential future improvements. Specifically you will develop a combination of technical competencies, professional and cognitive, academic and specific computer systems, digital logic and assembly language focused skills and knowledge

Algorithms and Mathematics

In this module you will develop a basic knowledge of algorithms and mathematics which can then be applied in cyber security domain. Algorithms are the building block of any software and as such skills to understand, design and develop algorithms are vital for IT professionals including cyber security professionals. You will subsequently be able to apply this knowledge and skill in your own context as a cyber security technical professional.

As such you will learn relevant computational Mathematics principles, models and terminologies required to solve the real-world problems and apply these in the context of cyber security.

Software Development

This module is designed to provide an introduction to the practical aspects of the development of a software application following a well-defined process and techniques. As such you will gain experience in the software development cycle, including requirement analysis, design, and implementation, and also learn to exploit implementation support technologies. Typical topics covered in the module include; software development methodologies such as waterfall, and Agile ; design tools such as Unified Modelling Language (UML) and object-oriented (OO) programming language and concepts of software testing.

Operating Systems and Server Administration

The operating system acts as an interface between user, application programs and computer hardware and is therefore considered as the most important component of computer systems. It performs a variety of functions including process management, memory management, file management, resource management, and security management. This module is designed to develop your introductory knowledge and skills in Operating System Security and Server Administration. As such the module will provide an opportunity for you to develop the skills and knowledge to understand the Operating System behaviour and its functions. This will help appraise and select the features of current Operating Systems and how they are configured and integrated to provide enterprise level services. Then the concepts of operating systems security will be introduced to equip you to develop techniques that are used to secure operating systems from hijacking, malicious bugs and viruses.

Human Computer Interaction and Cyber Security

In this module, you will develop an understanding of key theories, design issues and topics in Human Computer Interaction (HCI) and then apply them in the context of developing usable, interactive and secure computer systems. You will also develop prototypes in accordance to key usability standards and user needs. This module will also emphasise the technical aspects of prototyping and HCI. Typical topics covered in the module include; user-centred design, the design process, prototyping, and evaluating the user experience, etc. for the needs of multiple platforms

and emergent devices.

Professional Practice 1

In this module you will develop self-guided skills and knowledge related to your own professional development needs, and the context in which you are working.

Cyber Security is a wide field in which professionals can find themselves working within a number of different roles and specialisms, each requiring a specific technical skillset. Professional Practice 1 is an opportunity for you to tailor the learning conducted within Level 4 of your programme towards acquiring those skills that will help you develop towards becoming a Cyber Security Technical Professional.

Working with the module academic team and your employer, you will conduct a skills analysis to identify relevant training that can be undertaken. This training can take a number of forms, be it:

- Technical training delivered within the workplace, or class environment
- Structured online learning
- A mini project
- Or, another appropriate form approved by the academic team.

Following completion of the training, the acquired skills will be focused towards a specified project or business challenge. This should result in the development of a cyber security focused system, and its subsequent analysis, taking a holistic view to include the wider human elements of cyber security, and legal and ethical issues.

Level 5

Computer Security

This module will develop your knowledge and skills in Computer Security. You will subsequently be able to apply this knowledge and skill in your own context, and apply and analyse the implementation and recommend potential future improvements.

Specifically, the module aims to provide you with an overview of computer security techniques and fundamental knowledge of countermeasures. You will learn relevant cutting-edge computer security principles, models and terminologies require to secure modern computers.

Web and Mobile Application Security

This module is designed to develop fundamental knowledge and skills in web application and mobile security concepts. As such you will gain insights into different web and mobile security threats such as cross-site scripting (XSS), SQL injection, session hijacking. You will also learn how to apply essential security techniques to test and protect web and mobile applications from these

attacks. You will subsequently be able to apply this knowledge and skills in the design, implementation, testing and use of secure web and mobile applications and subsequently analyse their implementation and recommend potential future improvements.

Network Security

This module is designed to develop your knowledge and skills in network security principles, tools and techniques to proactively secure the perimeter against adaptive threat vectors. A blended learning approach of theory and practical explications will be used throughout the delivery.

As an Apprentice you will be exposed to hands-on exercises that emulate real-life scenarios in proactive network defence, monitoring and prevent strategies and be able to make better links to your existing work experience. You will subsequently be able to apply this knowledge and skill in your own context, and analyse the implementation in order to recommend potential future improvements.

Data Science and Cyber Security

The collection and use of large and diverse data set provide opportunities to businesses and organisations to gain useful insights for strategic decision making. This module is designed to develop your fundamental knowledge and skills in big data analysis for cyber security using algorithms and statistical analysis that deal with large diverse data sets. As such you will develop the skills required for maintaining data, efficient querying and accessing the data and adding semantic interoperability to meet cyber security objectives such as investigation and building intelligence and decision making. You will subsequently be able to apply this knowledge and skill in your own context, and subsequently analyse the implementation and recommend potential future improvements.

Ethical Hacking

This module is designed to develop your self-guided learning skills and knowledge and develop your own professional development needs in the context of your Degree Apprenticeship discipline and the context in which you are working. Cyber Security is a wide field in which professionals can find themselves working within a number of different roles and specialisms, each requiring a specific technical skillset. Professional Practice 2 builds on the skills developed so far to provide an opportunity for you to tailor the learning conducted within Level 5 of your programme towards acquiring those skills that will help you develop towards becoming a Cyber Security Technical Professional.

Working with the module academic team, your Skills Coach and your employer, you will conduct a skills analysis to identify relevant training that can be undertaken. This training can take a number of forms, be it:

- Technical training delivered within the workplace, or class environment
- Structured online learning
- A mini project
- Or, another appropriate form approved by the academic team.

Following completion of the training, the acquired skills will be focused towards a specified project or business challenge. This should result in the development of a cyber security focused system, and its subsequent analysis, taking a holistic view to include the wider human elements of cyber security, and legal and ethical issues.

Level 6

Digital Forensics and Incident Handling

This module is designed to develop your critical knowledge and skills in incident handling and digital investigations so as to exhibit awareness of the legal, ethical and professional implications and responsibilities for the digital investigator. As such you will learn to professionally acquire and analyse digital evidence utilising effective tools and techniques. You will subsequently be able to apply this knowledge and skill in your own context, and subsequently critically analyse the implementation and recommend potential future improvements.

Information Security Management

This module is designed to develop your critical knowledge and skills in Information Security Management principles and techniques that underpin the management of an organisation's information assets for which it is responsible. In doing so you will critically analyse the key concepts, theories, standards and frameworks of information security management, including risk assessment, people, resources, assets and processes to help organisations to reduce the likelihood of a data breach occurring and ways to limit their liabilities. This will enable you to evaluate an organisation's current approach to managing information security and to advise on the design and implementation of an appropriate strategy for managing an organisation's information assets to meet legal, regulatory, organisational and/or societal needs for information governance and security.

Cyber Offensive Defence

This module is designed to develop your critical knowledge and skills in Cyber Offensive Defence using Penetration Testing. You will subsequently be able to apply this knowledge and skill in your own context, and critically analyse its implementation, recommending potential future improvements.

Specifically you will develop a combination of technical competencies, professional and cognitive skills in Penetration Testing Methodologies & framework.

Cyber Security Project (30 credits)

This final applied research project is designed to present your critical knowledge, academic ability and skill in the field of Cyber Security. This will take the form of an individually negotiated project. Successful completion of the project is an essential requirement for your degree award.

As such you will learn how to engage with and critically review research literature and from this to develop relevant research objectives and questions as part of a research proposal. In addition, you will learn about, and be able to evaluate, different research methodologies and project management approaches open to you to work on your final project. On the basis of this, you will be able to make justified choices of research strategy and be able to use appropriate project management tools and approaches. You will also be equipped with the practical skills needed to execute and write up a coherent piece of research relevant to your degree. Through the module, you will be made aware of the ethical principles that govern cyber security research.

Specifically you will develop a combination of competencies, professional and cognitive, academic and specific in the cyber security field in order to apply the formal method of scientific enquiry, research and reporting. In this context, you will carry out a significant investigation in discovering new problem that requires an appropriate solution to be produced.

Professional Practice 3

This module is designed to develop your self-guided learning skills and knowledge and develop your own professional development needs in the context of your Degree Apprenticeship discipline and the context in which you are working. Cyber Security is a wide field in which professionals can find themselves working within a number of different roles and specialisms, each requiring a specific technical skillset. Professional Practice 3 is an opportunity for you to tailor the learning conducted within Level 6 of your programme towards acquiring those specialist skills that will help you develop towards becoming a Cyber Security Technical Professional.

Working with the module academic team and your employer, you will conduct a skills analysis to identify relevant training that can be undertaken. This training can take a number of forms, be it:

- Technical training delivered within the workplace, or class environment
- Structured online learning
- A robust research project
- Or, another appropriate form approved by the academic team.

Following completion of the training, the acquired skills will be focused towards a specified project or business challenge. This should result in the development of a cyber security focused system, and its subsequent analysis, taking a holistic view to include the wider human elements of cyber security, and legal and ethical issues.

Cyber Security Technical Professional End Point Assessment (10 credits)

The end-point assessment (EPA) is the culmination of your apprenticeship and gives you the opportunity to demonstrate that you have attained the skills, knowledge and behaviours set out on the Cyber Security Technical Professional standard. Passing the EPA is a requirement in order to complete the BSc (Hons) programme. There are two parts to the end-point assessment:

(a) A Practical Test (this will consists of four exercises to be assessed against the defined set of knowledge, Skills and Behaviours).

(b) A Technical Discussion (informed by a portfolio).

Prior to attempting the EPA you will have met the following requirements;

1. Passed all the other modules in the BSc (Hons) Cyber Security Technical Professional degree; and
2. the employer confirms that the apprentice is ready for the EPA and has met the knowledge, skills and behaviour requirements set out in the occupational standard; and
3. completed e-portfolio (which may be digital or online) in relation to the skills, knowledge and behaviours set out in the apprenticeship standards, on which the substance of the EPA technical discussion shall be based. The Technical Discussion is based on the Portfolio of evidence developed throughout the apprenticeship and is used to map your achievement against the apprenticeship standard. You will be provided with guidance on preparation for the EPA and the specific details of the assessment requirements; and
4. the apprentice has passed Level 2 English and maths (if not already achieved);

Full details of the EPA can be found on the apprenticeship standard website.

The course information published on this page is accurate for the academic year 2021/22 and every effort is taken to ensure it is kept up to date. We aim to run the course as advertised however, changes may be necessary due to updates to the curriculum (due to academic, industry or apprenticeship standard developments), learner demand or UK compliance reasons.

Learner Support

Skills Coach

Your Skills Coach will be your primary, non-academic contact, supporting you in the successful progression and completion of your apprenticeship. Your coach will support you in reviewing your progress and collecting evidence of your practice at work to integrate into your module assessments and final endpoint project/assessment. They are also a point of contact for queries, concerns, or general support.

Your Coach can help you with:

- Coaching and supporting work-based learning activities
- Reviewing your progress with your apprenticeship portfolio progress
- Help with achieving your EPA
- Advice and guidance on mitigating (extenuating) circumstances processes and potential breaks in learning.

Workplace Mentor

A Workplace Mentor will be appointed by your employer and typically would be someone you work with. Your workplace mentor will be familiar with the apprenticeship programme and its workplace requirements. They will facilitate the workplace learning opportunities to enable you to meet the requirements of the degree apprenticeship standard.

ACE Team

They are the Academic Community of Excellence (ACE) Team, and amongst the team, have many years of experience providing academic guidance to students on subjects such as how to write in an academic style, how to read smarter rather than longer and how to reference accurately.

The ACE Team will provide you with support on academic matters outside of the classroom. You can also book 1-1 meetings (mainly online) with the ACE Team and get feedback on your academic style of writing, references and critical report writing.

How can the ACE Team support you?

1. “Welcome to the World of Academia” online workshops: if you wish to have an introduction to or a review of the different aspects of academic life before starting your programme, then please do join their online workshops (non-obligatory – but much to be gained from joining!).
2. One-to-one tutorials: you can book a virtual 30-minute tutorial to discuss your academic development skills, such as paraphrasing, referencing and academic writing.
3. Online workshops: we offer ongoing support workshops on a variety of academic subjects such as structuring an argument, academic style and criticality.
4. Our own-created range of learner materials: we have also developed a wide range of ACE Team created materials based on common questions and academic needs.

QA Welfare Services

Our Student Welfare Team is on hand to assist you throughout your studies. Some degree apprenticeship learners have additional learning needs which the Welfare Team can assist with, or they might help you with personal circumstances that are affecting your studies.

Entry Requirements

-

- 120 UCAS points through A-levels or equivalent
- In order to attempt the EPA apprentices must have achieved GCSE Maths and English at Grade C – you may still enter the programme but will need to evidence Level 2 Maths and English qualification before starting the gateway and EPA

Non-standard entry requirements

Applicants who can in other ways demonstrate their ability to benefit from the programme, in particular mature students without formal qualifications, will always be considered and will be invited to contact the Programme Leader to discuss their application. The University welcomes applications from students studying qualifications from different qualification types – for example A level and a BTEC qualification in combination, and if you are made an offer you will be asked to achieve UCAS Tariff points from all of the qualifications you are studying at level 3.

A good GCSE profile is expected including English Language and Mathematics at minimum grade C (or a University recognised equivalent). Apprentices without Level 2 English and maths must achieve this prior to taking the end-point assessment. If you have studied for a new GCSE for which you have achieved a numerical grade then you will be required to achieve a minimum grade 4.

Informal Interviews

Informal interviews will be held where

- The suitability of a candidate is in doubt and further evidence is sought.
- The candidate presents an unusual set of qualifications taken or pending, and an appropriate conditional offer needs to be determined.
- Candidates may need advice on the appropriateness of the programme.

Applicants invited for an informal interview will always be informed of its purpose.

End Point Assessment

You must be able to evidence level 2 English and Maths before you start your End Point Assessment. You may still be begin the programme without these but must obtain the qualifications in order to begin the EPA.

Fees & Finance

There is no cost to you as a degree apprentice. Degree Apprenticeships are fully funded by the Apprenticeship Levy through your employer.

If you’re an employer, the total funding for this programme is:

- £24,000

Travel expenses to travel to QA centres should be covered by the employer.

All textbooks are provided free of charge as e-books. Any students wishing to use paper copies will need to pay for these themselves.

How to apply

If you are interested in applying to study or to offer a Degree Apprenticeship, please complete the enquiry form on this page and one of our account managers will be in touch.

In order to join a Degree Apprenticeship, the employer will either recruit new staff or select existing staff that are suitable for the programme.