3 year BSc (Hons) Full-Time Degree

4 ½ year BSc (Hons) Higher Level Apprenticeship Degree

BSc (Hons) Cyber Security and Networking Infrastructure

Validated by The Open University

Contents

Overview of Northern Ireland IT Employment Sector

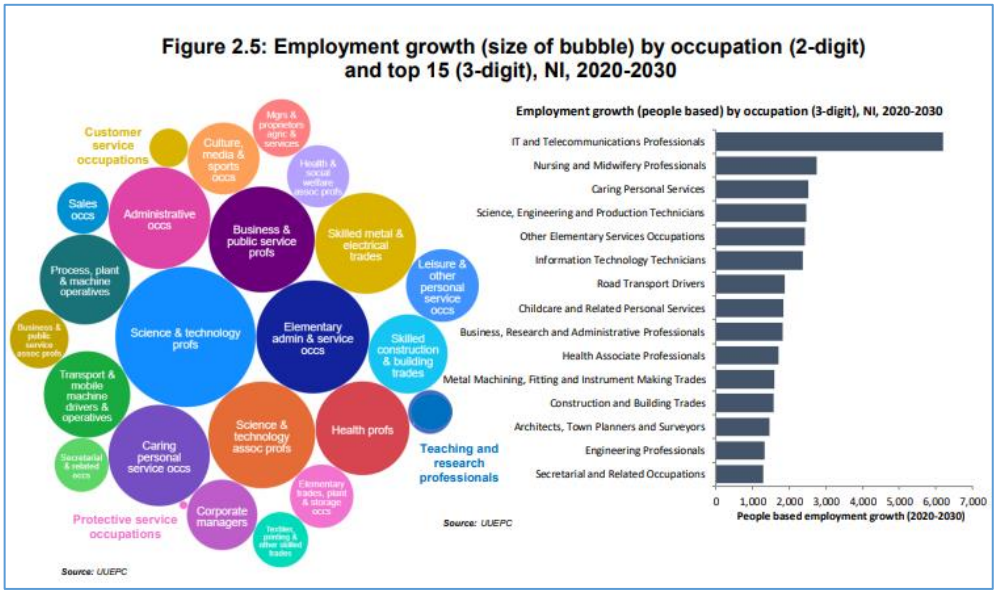
Belfast Met offers two BSc (Hons) Degrees in IT at the Castlereagh Campus. These programmes align themselves to research carried out on the economic and technical future of Northern Ireland.

The Northern Ireland Digital Matrix Report of 2016 (http://matrixni.org/reports/2016-digital-ict/) proposed the following opportunities for Northern Ireland within the digital arena.

Opportunities for Northern Ireland

- **Advanced networking:** the increased capability to move large amounts of data anywhere, quickly and reliably changes where economic activity is located.
- **Applications:** more sophisticated applications are replacing human activity in lower-skilled ICT work.
- **Data analytics:** understanding of transactional data can lead to changes in the location of business functions, from manufacturing to provision of IT services; and automation of data analysis changes the pattern and location of business processes.
- **Cyber security:** as organisations rely increasingly on networks and cloud-based services running on virtualised infrastructure, securing data becomes harder.
- **New ICT service models:** the rise of cloud-based applications mean that IT services are no longer delivered from data centres close to the point of use, and sometimes from unknown locations.

Analysis into employment growth from 2020 to 2030 is reported in the Northern Ireland Skills Barometer Report 2021. The key findings stated in the report are, “the occupation with the largest growth over the next decade is forecast to be IT and telecommunications professionals (6.2k) sector, and indirectly linked to an increased demand for digital skills across the wider economy.”



The report also investigates the expected labour demand by occupation with the biggest demand occupation is science and technology professionals.

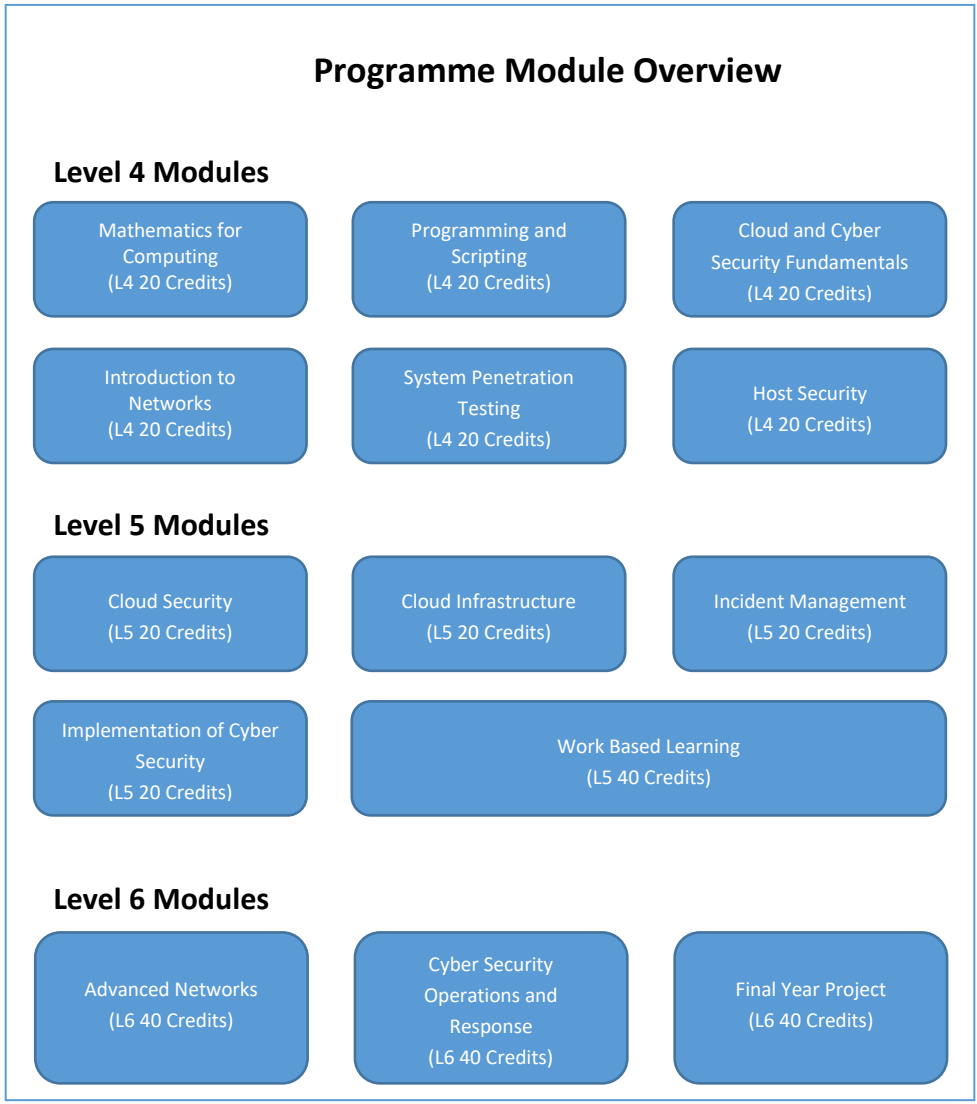
This is directly linked to the growth of the ICT. With this in mind, Belfast Metropolitan College has created Full Time and Higher Level Apprenticeship Degree programmes that addresses the need for a skilled workforce in the areas of Cyber Security, Networking, Data Analytics and Software/Cloud development.

The two Foundation Degrees that aim to cover all of the areas identified in the NI Digital Matrix report and the Skills Barometer are: -

- **Foundation Degree in Cyber Security with Cloud and Network Infrastructure**
- **Foundation Degree in Software and Cloud Development with Data Analysis**

Both these programmes have an optional 1-year BSC (Hons) Top-Up, that students who have successfully achieved an IT related foundation degree can enrol onto.

BSc (Hons) Degree in Cyber Security and Networking Infrastructure (validated by The Open University)



Modules Overview

Level 4 Modules

Introduction to Networks (20 credits)

This module is an introduction to computer networking. Students will become familiar with computer networks; configuring network devices and simulating networks using software. They will also analyse network design and device configuration to resolve problems in a simple computer network and learn to utilise fault-finding techniques to diagnose faults. This module is aligned to Cisco CCNA 1.

Cloud and Cyber Security Fundamentals (20 credits)

This module introduces the core Cloud and Cyber security concepts, skills, and technologies. Candidates will cover a wide range of activities and themes such as Cyber Security, Cloud Computing, in relation to business processes, financial considerations, project management, as well as Cyber security within networking both on/off premises with legal compliance relevant to industry application.

Programming and Scripting (20 credits)

This module will provide students with a basic knowledge of the techniques used in program development. Students will learn the concepts of good program design and subsequent successful implementation. This module will make students aware of the basic building blocks used in developing and testing simple maintainable programs. This module will provide an introduction to programme scripting.

Host Security (20 credits)

This module will provide students with a basic knowledge of computer security. Students will learn about the major challenges to computer security and subsequent ways of

protecting systems and data against various types of vulnerabilities, threats and attacks and the legal, privacy and ethical issues in computer security.

System Penetration Testing (20 credits)

This module will provide students with an understanding of both theory and practical techniques in the field of Systems Penetration Testing and will underline the importance of adhering to UK and international regulations whilst carrying out Systems Penetration Testing.

Mathematics for Computing (20 credits)

This module provides students with a mathematical background to support and enhance material presented in computer science modules. Students will develop proficiency in the use of fundamental mathematical concepts in the areas of discrete structures, algorithms and complexity. Students will also develop an ability to absorb further specific mathematical knowledge as required for given specialised areas. The analytic skills and conceptual thinking required for competence in areas such as programming, database analysis, formal specification, encryption and systems design are developed in the module.

NB Students can exit Level 4 with a Certificate in HE on successful completion of the six Level 4 modules.

Level 5 Modules

Cloud Security (20 credits)

The aim of this module is to provide students with a critical understanding of security threats against cloud computing systems and the security measures designed to protect such systems. The module will explicitly develop students' knowledge and experience in the design and application of cloud security solutions. The module will also equip students with the knowledge and skills required for further academic study and future employability in the area of computer security.

Cloud Infrastructure (20 credits)

This module provides an in-depth understanding of cloud infrastructure and architecture. The module will also compare and analyse various cloud infrastructure architecture technologies and the impact on various operating systems and platforms. Technical challenges and recent advances will also be discussed. The module will also lay out possible future trends for cloud infrastructure. In this module students will also look at environmental impact of the cloud and job roles.

Incident Management (20 credits)

The module will cover incident management from a tactical/regional and national/strategic perspective using the four-stage model: Identification, preparation, mitigation, and recovery.

A range of actual and potential incidents will be covered with primary focus within Cyber-attacks as well as including an understanding of other types of attacks that could be used in association with a cyber-attack such as air accidents, marine accidents, rail accidents, terrorist attacks, and industrial, nuclear and chemical incidents.

Implementation of Cyber Security (20 credits)

This module will teach learners the knowledge and skills necessary to identify risk, to perform risk mitigation activities, provide infrastructure, application, information, and operational security. Learners will learn to apply security controls to maintain confidentiality, integrity, and availability. Learners will identify appropriate technologies and products, troubleshoot security events and incidents, and operate with an awareness of relevant policies, laws, and regulations.

Worked Based Learning (40 credits)

This module will enable students to apply their Cyber Security and Networking Infrastructure knowledge and skills in their working environment where as employees they will have been exposed to a range of the practices and tools used by the Computing Infrastructure sector. As they are based in a relevant and supervised employment this will allow them, the opportunity to apply and develop their skills and knowledge gained throughout the course. While working as a Computing Infrastructure engineer they will also have the opportunity to enhance their personal development and interpersonal skills.

NB Students can exit Level 5 with a Foundation Degree on successful completion of the six Level 4 modules and five Level 5 modules.

Level 6 Top-Up Modules

Advanced Networks (40 credits)

The aims of this module are: -

- Provide students with an understanding of further switching technologies such as Spanning Tree Protocol (STP), Per VLAN Spanning Tree Plus Protocol (PVST+), and link aggregation and how to configure and troubleshoot them.
- Understand, configure, and troubleshoot first hop redundancy protocols in a switched network.
- Understand, configure, and troubleshoot wireless routers and wireless clients
- Configure and troubleshoot routers in a complex routed IPv4 or IPv6 network using advanced routing protocols.
- Understand and configure DHCP.

Cyber Security Operations and Response (40 credits)

The aims of this module are: -

- Security Operations and Management.
- Understanding Cyber Threats, IoCs, and Attack Methodology.
- Incidents, Events, and Logging.
- Incident Detection with Security Information and Event Management (SIEM).
- Enhanced Incident Detection with Threat Intelligence and Incident Response.

Final Year Project (40 credits)

This module will enable students to apply their knowledge and skills gained throughout the course and combine them into industry relevant projects as seen in the working environment. Combining different aspects of the subject areas previously studied in the

course will empower students to develop skills that suit their preferred interests and will present the opportunity for students to be exposed to a range of the practices and tools used by relevant industry.

NB Students successfully completion the three Level 6 modules will be awarded the BSc (Hons) in Cyber Security and Networking Infrastructure Top-Up Degree.

Additional qualifications offered with programme

The following vendor qualifications are offered for free along with the course modules.

Microsoft Azure Fundamentals (AZ-900)

This exam measures students' ability to accomplish the following technical tasks: develop Azure Infrastructure as a Service compute solutions; develop Azure Platform as a Service compute solutions; develop for Azure storage; implement Azure security; monitor, troubleshoot, and optimize solutions; and connect to and consume Azure services and third-party services.

Cisco Cyber Security Essentials

The Cybersecurity Essentials course develops foundational understanding of cybersecurity and how it relates to information and network security. The course introduces students to characteristics of cyber-crime, security principles, technologies, and procedures to defend networks.

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

The exam covers the fundamentals of security, compliance, and identity (SCI) across cloud-based and related Microsoft services and the objectives are to help students understand how Microsoft security, compliance, and identity solutions can span across these solution areas to provide a holistic and end-to-end solution.

CompTIA Security+

CompTIA Security+ is a global certification that validates the baseline skills you need to perform core security functions and pursue an IT security career.

CompTIA Network+

CompTIA Network+ is a performance-based certification that helps you develop a career in IT infrastructure by validating the hands-on skills needed to troubleshoot, configure, and manage both wired and wireless networks.

CompTIA Pentest+

CompTIA PenTest+ is a certification for intermediate level cybersecurity professionals who are tasked with penetration testing to identify, exploit, report, and manage vulnerabilities on a network. CompTIA PenTest+ assesses the most up-to-date penetration testing, and vulnerability assessment and management skills necessary to determine the resiliency of the network against attacks.

Cisco Certified CyberOps Associate

The exam measures a student's knowledge of security concepts, common network and application operations and attacks, and the types of data needed to investigate security incidents. This course teaches students how to monitor alerts and breaches, and how to understand and follow established procedures for response to alerts converted to incidents

Entry Requirements

Applicants must:

Hold 200 UCAS points or 80 tariff points (e.g. CDD or BB at A-Level or MPP at Level 3 Extended Diploma), GCSEs at C or above in English and Mathematics, or equivalent qualifications, such as Level 2 Essential Skills in Numeracy and Literacy.

Full-Time Costs and Duration

Course Fees: - £2765 (each year). Subject to change. Student finance available

Applications open November 2022

Duration: 3 years

Start Date – September 2023

End Date - June 2026

Hours per Week – 16 hours per week.

Campus - Castlereagh

Higher Level Apprenticeship Costs and Duration

Course Fees: - £0

Recruitment/Applications open 28th April 2023

Duration: 4 ½ years

Start Date – November 2023

End Date - May 2028

Hours per Week – 7 hours day release at the college, 2-4 days a week at employer.

Campus - Castlereagh

Contact Details

Cyber Security with Cloud and Network Infrastructure (Full-Time)

Oisin Scullion oscullion@belfastmet.ac.uk

Dr Jonathan Doherty jonathandoherty@belfastmet.ac.uk

Cyber Security with Cloud and Network Infrastructure (Apprenticeship)

Steven Barr sbarr@belfastmet.ac.uk

Castlereagh Campus

Castlereagh Campus
Montgomery Road
Belfast
BT6 9JD

Tel: 028 9026 5000