MASTER OF SCIENCE IN CYBERSECURITY

FACTFILE

Spread the cost with our direct debit plan

Application
Apply online at www.ncirl.ie

Part-time Schedule

Duration
2 years; 4 semesters with a final internship/practicum.

Delivery
Blended - Livestream with some on-campus stream classes , scheduled in advance.

Start Date
Sept 2024

Indicative Timetable
Two evenings per week, 18.00 - 22.00 and every second Saturday

Fees
€4,700 per annum
€9,400 total fee
(Fees revised annually)

Full-time Schedule

Duration
1 year; 3 semesters with a final internship/practicum.

Delivery:
Campus – Classes will take place face-to-face on campus.

Start Date
Sept 2024 and Jan 2025

Indicative Timetable
Students need to be available 09.00-18.00 Mon – Fri. Class days and times vary.

EU Fee
€6,800 total fee
(EU/Ireland applicants)
(Fees revised annually)

Course Description

Cybersecurity is an essential need for a modern society in which information technology and services pervade every aspect of our lives. Cybersecurity has the fastest growth rate among all areas of IT, with the labour market encountering a severe workforce shortage in this field.

The aim of this programme is to provide learners with essential expert technical knowledge, competence and skills of the most important technical concepts of cybersecurity and how they are applied in areas such as device, network, cloud, web and application security.

The course is technical and practical in nature, uniquely embedded in industry, and develops in-depth expertise of core technical topics within the cybersecurity area. The programme emphasises the development of technical and research skills in the cybersecurity area through analysis, investigation, requirements elicitation, problem solving, and teamwork. In addition, emphasis is placed on the study of the latest appropriate technology and techniques necessary for the cultivation of advanced investigative skills.

Who is the course for?

This course is ideal for ICT professionals or graduates with an honours degree in computing or in a cognate area (STEM) who wish to develop a career as a cybersecurity professional; to take a leading technical or managerial role; to progress faster in their employment or to apply the knowledge in their current role. Candidates who do not hold a computing degree and are currently working in the IT sector may be considered, based on relevant academic qualifications or extensive work experience.

As a graduate of this course, you will be able to:

- Critically assess and evaluate ethical, legal, privacy, sustainable, and governance issues associated with the management of data assets in the cybersecurity domain.
- Communicate effectively complex and advanced cybersecurity concepts to a range of audiences in both written and verbal media.
- Apply advanced security knowledge and utilise practical skills and technologies to design and implement cybersecurity solutions that address business and technical problems.
- Make decisions and address security requirements through analytical thinking, communication, and interaction.
- Analyse, identify, and document measures to address vulnerabilities, risks, weaknesses, and other safety aspects within a given cybersecurity context.
- Identify knowledge gaps and undertake self-learning to acquire new knowledge and meet the requirements of the rapidly developing and expanding cybersecurity industry.
- Conduct independent research in the cybersecurity area and formulate and implement novel ideas by applying the latest research methodologies and industry practices.

Award and Progression

The Master of Science in Cybersecurity is awarded by QQI at level 9 on the National Framework of Qualifications (NFQ). Students who successfully complete this course may progress to a major award at level 10 on the NFQ. Students may also elect to exit early with a Postgraduate Diploma in Science in Cybersecurity at level 9.

Career Prospects

Several reports indicate shortage of skills and strong demand for cybersecurity professionals. The Expert Group on Future Skills Needs identified cybersecurity as a high-growth area that requires significant support for skills development. The State of the Cybersecurity Sector in Ireland 2022 Report indicates that there are almost 500 companies offering cybersecurity services or have employees in internal cybersecurity roles, and 83% of companies expect to grow their cybersecurity team over the next 12 months. This field has the fastest growth rate

following roles: information security analyst, secure application developer, cybersecurity tester, risk analyst / consultant, cyber incident responder, cloud security analyst, security researcher, etc.

Entry Requirements

An honours (level 8) primary degree in computing or a cognate area with a 2.2 award or higher. Cognate area means a STEM (Science, Technology, Engineering, and Mathematics) degree that also has taught programming/application development related modules. Candidates are expected to have programming ability, which can be demonstrated through transcripts, recognised certifications, and/or relevant work experience. An assessment and/or interview may be conducted to ascertain suitability, if necessary, for candidates who do not meet the normal academic requirements.

The College operates a Recognition of Prior Experiential Learning (RPEL) scheme meaning applicants who do not meet the normal academic requirements may be considered based on relevant work and other experience. This may be assessed using a portfolio of learning, demonstration of work produced, and an interview. The programming ability of the applicant will also be assessed. Non-English-speaking applicants must demonstrate fluency in the English language as demonstrated by an IELTS academic score of at least 6.0 or equivalent.

Laptop Requirement

This programme has a BYOD (Bring Your Own Device) policy. Specifically, students are expected to successfully participate in lectures, laboratories and projects using a portable computer (laptop/notebook) with a substantial hardware configuration. The minimal suitable configuration is 8GB of RAM (16GB are recommended); a modern 64-bit x86 multi-core processor (Intel i5 or superior); 250+ GB of available space in hard disk; WiFi card; and a recent version of Ubuntu, macOS, or Windows.

It is the responsibility of each student to ensure their computer is functioning correctly and that they have full administrator rights. NCI IT cannot provide support for these personal devices.

Some students may be able to avail of the Student Laptop Loan Scheme, subject to eligibility. See page 87 for more information.

COURSE CONTENT

Core Modules

- Network Security and Penetration Testing
- Security Fundamentals
- Data Governance, Ethics, and Sustainability
- Cloud Architectures and Security
- Cryptography and Blockchain
- AI/ML in Cybersecurity
- Business Resilience and Incident Management

Elective Modules

- Secure Web Development
- Forensics and eDiscovery
- Secure Application Development
- Malware Analysis

Note that there are dependencies between secure development electives. To study Secure Application Development in semester 2, students must have studied Secure Web Development in semester 1. However, all students can elect to study Malware Analysis in semester 2.

Research Elective

- Practicum
  or
- Internship

Elective modules are subject to availability and a minimum number of students required to run a module.

Assessment

The course will be assessed with a blend of continuous assessments and/or project work and/or exams. This varies between modules but typically assessment is 40% continuous assessment and 60% project or exam. Please note that in some instances exams may take place in the daytime, evenings and at weekends.