Postgraduate Diploma in Science in Cybersecurity

(Blended/Online Directed E-Learning) (1 Year)

STUDY ANYWHERE IN IRELAND

This is a blended/online learning course that features Directed E-Learning activities such as live online classroom sessions and tutorials/videos on the College's e-learning system. This allows for online class time to be interactive, practical, and focused, with theory-based content being covered outside of class time with self-paced tutorials/videos, and practical content being covered in live online classes with support from lecturers and lab assistants. At certain limited and pre-scheduled times there will be opportunities for on-campus sessions. These on-campus sessions will also be dual delivered so students who do not wish to attend campus for these sessions will have the option of attending them online.

Location: Online (with limited classroom sessions)

Start Date: The course is expected to start in the week commencing 22nd January 2024

Indicative Schedule: Tuesday and Thursday 18.00 - 22.00.

There will also be 4.5 hours self-paced learning per week on NCI's Learning Platform weekly. This will not appear on your timetable.

Career Bridge classes will be delivered one day per week in Semester 2 from 17.00 to 18.00. Day to be confirmed.

Duration: January to May 2024, May to August 2024 and September to December 2024

Applications: Apply online at www.springboardcourses.ie

Fees: A student contribution fee of €695 is applicable if you are in employment. No fees applicable if you are unemployed.
The scheme does not cover any allowance for books and materials.

If a student contribution fee is applicable this must be paid in full no later than 8th March 2024.

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.

Career Prospects

Several reports indicate a 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 when compared with the rest of technology jobs. Considering the high demand of various types of jobs in the cybersecurity domain that currently exist in the market, graduates from this course may work in the following roles: information security analyst, secure application developer, cybersecurity tester, risk analyst / consultant, cyber incident responder, cloud security analyst, security researcher, etc.

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) that 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.

Award and Progression

The Postgraduate Diploma in Cybersecurity is awarded by QQI at level 9 on the National Framework of Qualifications (NFQ).

Students who successfully complete this course can optionally complete the additional 30 credits required to upgrade their qualification to the MSc in Cybersecurity (Not included under Springboard+, additional fee would apply).

Academic 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 Requirements

This programme has a BYOD (Bring Your Own Device) policy. Specifically, students are expected to successfully participate in lectures, laboratories and projects using a laptop computer with a substantial hardware configuration. A suitable configuration is 8GB of RAM (16GB are recommended); a modern 64-bit x86 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 the student to ensure their laptop is functioning correctly and that they have full administrator rights to the machine.

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

Free Laptop loan for eligible students on this course:

Students who are eligible for HEA funding for this course may also be eligible for a free laptop provided on a loan basis for the duration of the programme. This will be a suitable specification machine for completion of the programme but must be returned once you have finished your course. Overall numbers of laptops available are subject to maximum numbers and no other alternatives can be offered.

Check *https://www.ncirl.ie/Students/Student-Services/Support-Services/Student-Laptop-Fund* for updates on the next opening date for applications.

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.

Course Content
(Blended/Online Delivery)
(1 Year)

The course offers two specialisations: Forensics and Cloud Security. Learners must select one specialisation. Specialisations will only run due to student demand.

Semester 1

- Security Fundamentals
- Data Governance, Ethics, and Sustainability
- Secure Web Development (Elective)
- Forensics and eDiscovery (Elective)

Semester 2

- Network Security and Penetration Testing
- Cryptography and Blockchain
- Secure Application Development (Elective)
- Malware Analysis (Elective)
- Career Bridge

Semester 3

- Cloud Architectures and Security
- AI/ML in Cybersecurity
- Business Resilience and Incident Management

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.

Electives will run subject to learner demand. Learners will be asked to choose their specialisation before programme commencement.

Springboard Careers Advisors will proactively support you to find relevant employment during the course or following the completion of the course.

*Note that all modules count towards the final award classification.