Est. 1841 | YORK ST JOHN UNIVERSITY

Programme Specification

BSc (Hons) Cyber Security

BSc (Hons) Cyber Security with a year in industry

School:	Science, Technology and Health
Subject area:	Cyber Security
Entry from academic year:	2022-23
in the month(s) of	September
Awarding institution:	York St John University
Teaching institution:	York St John University
Delivery location:	York St John University
Programme/s accredited by:	
Exit awards:	Certificate of Higher Education Computer Science Diploma of Higher Education Cyber Security Diploma of Higher Education Cyber Security with a year in industry BSc (Ord) Cyber Security BSc (Ord) Cyber Security with a year in industry
UCAS code / GTTR / other:	I100
Joint Honours combinations:	Not applicable
QAA subject benchmark statement(s):	Computing (October 2019)
Mode/s of study:	full time for 3 years part time for 6 years full time for 4 years (with year in industry)
Language of study:	English
Paired with Foundation Year	No
Study abroad opportunities:	No
Opt-in YSJU Placement Year opportunity:	Yes

Introduction and special features

Cyber security is a growth area, and this programme will offer cyber security modules in areas that are seeing high interest and growth in the industry and academia. The programme will provide you with an excellent opportunity to become a competent and confident cyber security expert with in-depth knowledge of theory, concept, and hands-on cyber security skills and provide you with cognitive, practical and transferable skills needed for a successful cyber security career.

The programme's content is designed to equip you with the knowledge and understanding of essential facts, and deploying appropriate practices, policies, and tools to specify, design, implement and evaluate cyber security systems. As a student of this programme, you will be provided with the necessary technical and higher-level reasoning skills, qualities, and transferable skills essential for employment and further study. The awareness of professional standards, codes of conduct, and relevant legislations are embedded in the

module content and practice. You will be encouraged to gain professional certifications and register for professional bodies membership to promote your commitment to professional standards.

The programme is designed to provide you with a rigorous education in core cyber security subjects, including Information Security Management, Penetration Testing, and Vulnerability Assessment, Network Security: Attacks and countermeasures, Data Privacy, the Internet of Things, with optional modules in Digital Forensics, Cloud Security Privacy & Compliance, and Risk & Information Systems Control. To encourage the consolidation of knowledge, you are offered continual opportunities throughout your study to apply learned skills through a series of 'live' projects that engage real-world challenges. This experience of real-world testing is enhanced in level 5 through the Continuing Professional Development (Professional and Research Practices) module, allowing you the opportunity to immerse and test yourselves in either a commercial environment or a self-initiated entrepreneurial project.

In addition to specific knowledge and skills, you will be supported to develop key professional attributes through a number of activities including reflection on work-based practice to re-enforce your critical skills, addressing complex real-world situations through problem-based learning.

Offensive Security (https://www.offensive-security.com/why-offsec/), one of the leading penetration testing organizations, was consulted to explore ways of making it easier for students and staff to earn the industry-leading pen-testing certificates, and to inform the programme's curriculum with the contents and certifications of the industry-leading courses.

Special features of our programme

Some of the programme's uniqueness around teaching and learning strategy includes a practical degree, with a small number of students per session/class with practical content and research elements; the assessment strategy mainly focuses on portfolio and industry-related project-based assessments.

Inclusivity within the programme: the practical learning platforms are primarily virtual lab resources, dedicated cyber security hardware, and software that are free and open-source to enable you to practice your learning at your convenience with less effort and at any time and place.

Dedicated Resources: you will study in our dedicated workspace, which serves as home "base" for our students - each level has their specialist labs with specialised hardware and software resources, including our virtual lab resources on a dedicated/separate network allowing you to carry out the required cyber security tasks.

CPD: As part of your continuous professional development, you will be offered professional certification courses and participation, including Microsoft certificates with access to the Microsoft tools and materials. Alongside your degree qualification, you will also be supported to obtain industry-recognised certifications for various technologies to augment your degree and validate your skills needed to succeed across various cyber security careers.

Learning support: You will be supported with appropriate learning resources including academic, administrative, and technical staff, dedicated computing and communication facilities which include software tools, and specific and general learning facilities including access to appropriate digital and print-based information and effective academic advice and guidance.

A year in industry: With options to study full or part-time; to select a programme with or without a year in industry, there are a lot of options to choose the study mode which suits you. During the year in industry placement, you will be allocated a mentor from within the University, who will monitor your progress throughout the placement. This may include Skype/email conversations. You will have a minimum of one field visit which will include a conversation with the employer.

In addition to specific knowledge and skills, you will be supported to develop key professional attributes through identifying suitable methods and implement principled solutions within a professional, legal, and ethical framework to address issues including data management and use, security, EDI, and sustainability and entrepreneurship. You will be supported to develop your skills through several activities including

reflection on work-based practice to re-enforce your critical skills, addressing complex real-world situations through problem-based learning.

Sustainability: You will be introduced to a new practice of computational sustainability by building environmental and social sustainability projects and applications using computer science principles, methods, and tools and the use of open, private, and public cloud services, learning environments, and data. You will study modules such as Artificial intelligence, Data Analytics for Big Data analytics, and Internet of Things paradigms for building Cyber-Physical system applications.

Future focussed: our Cyber Security programme will provide you with subject-specific and key transferable skills and a creative and ethical approach to your cyber security career, equipping you with the critical and analytical knowledge to play your part in shaping the future.

The programme will provide:

- The ability to apply practical and analytical skills.
- The ability to self-manage a significant piece of work.
- Critical self-evaluation of the process.
- An underpinning of computation as a creative problem-solving practice.
- A focus on formative philosophical discourses – ethics.
- A balanced focus on technical theory, practice, and ability to recognise the legal, social, ethical and professional issues around the subject.
- An involvement in substantial individual and group projects.
- Integrated professional practice and certifications opportunities.
- Live projects working with and to industry specifications.
- Team working opportunities throughout which mirror and prepare you for working in industry.

Admissions criteria

You must meet the University's general entry criteria for undergraduate study.

If your first language is not English, you may need to take an IELTS test or an equivalent qualification accepted by the University (see https://www.yorksj.ac.uk/international/how-to-apply/english-language-requirements/).

If you do not have traditional qualifications, you may be eligible for entry on the basis of Recognition of prior learning (RPL). We also consider applications for entry with advanced standing.

Programme aim(s)

The purpose of this programme is to provide you with an excellent educational experience with the necessary technical and higher-level reasoning skills that enable you to become a Cyber Security expert/specialist, with the cognitive, practical, and transferable skills needed for a successful cyber security career.

Programme learning outcomes.

Upon successful completion of the programme, you will be able to:

Level 4

4.1 Demonstrate the ability to deploy appropriate theory, practices and tools for the specification, design, implementation, and evaluation of computer-based systems and security.

4.2 Demonstrate knowledge and understanding of essential facts, concepts, principles, and theories relating to computer applications and security.

4.3 Recognise and analyse criteria and specifications appropriate to specific problems, and plan strategies for their solution.

4.4 Demonstrate basic creative problem-solving skills as applied through Computer Science and the use of knowledge and understanding in the modelling and design of computer-based systems and security.

4.5 Demonstrate the ability to analyse the extent to which a computer-based system meets the criteria defined for its current use and future development.

4.6 Demonstrate an understanding of the link between theory and practice and ability to recognise and analyse criteria and specifications appropriate to specific problems, and plan strategies for their solution

Level 5

5.1 Recognise the legal, social, ethical, and professional issues relating to computing technology and appropriate professional, ethical and legal practices, and standards.

5.2 Analyse, evaluate, and develop organisational cyber security architecture and standard that includes network, physical and process controls, and applications, that can be implemented across an organisation to reduce information and systems risk, identify, and mitigate the vulnerability, and ensure organisational compliance.

5.3 Recognise any risks or safety aspects that may be involved in the operation of computing and information systems and security within a given context;

5.4 Apply appropriate theory, practices, and tools for the specification, design, development, and evaluation of intermediate computing systems, including the application of computing in scientific conclusions and legal decision-making.

5.5 Apply the principles, methods, and tools of computing and information security to design, develop and manage information systems that meet business needs

5.6 Demonstrate critically knowledge and understanding of methods, techniques and tools for information modelling, management, and security.

Level 6

6.1 Apply and critically analyse the concepts of design, defensive programming and testing and their application to build robust, resilient systems that are fit for purpose;

6.2 Employ practical skills to develop advanced application to solve a real-life problem with a critical evaluation of diligence to standards for secure system design, legal and ethical concerns;

6.3 Apply a high level of project management skills, technical knowledge, and creative techniques to the production of a final computer science project & report;

6.4 Engage with contemporary scholarship utilising research methodologies and deploying analytical skills to sustain a coherent intellectual critique on particular aspects of computer science and allied fields;

6.5 Deploy effectively the tools used for the construction and documentation of secure computer applications, with particular emphasis on understanding the whole process involved in the effective deployment of secure computer system and applications;

6.6 Define a problem, research its background, understand the social context, identify constraints, understand customer and user needs, identify, and manage cost drivers, ensure fitness for purpose and manage the design process and evaluate outcomes;

6.7 Use appropriate theoretical and practical processes to specify, design, deploy, verify, and maintain information systems, including working with technical uncertainty.

Programme structure

Code	Level	Semester	Title	Credits	Module status	
					Compulsory (C) or optional (O)	non-compensatable (NC) or compensatable (X)
COM4009M	4	1	Programming 01	20	C	X
COM4010M	4	1	Maths and Problem Solving	20	C	X
COM4011M	4	1	Security Systems and Products	20	C	X
COM4012M	4	2	Programming 02 – Programming for the Web	20	C	X
COM4013M	4	2	Operating Systems	20	C	X
COM4014M	4	2	Software Engineering	20	C	X
COM5012M	5	1	Programming 03 – Systems Programming and Scripting	20	C	X
COM5013M	5	1	Database Systems	20	C	X
COM5014M	5	1	Computer Networks	20	C	X
COM5026M	5	2	Digital Forensics	20	C	X
COM5016M	5	2	Professional and Research Practices	20	C	X
COM5017M	5	2	Information Security and Risk Management	20	C	X
COM5018P	5	1&2	Year in Industry	0	C if year in industry	NC if year in industry
COM6016M	6	1+2	Dissertation	40	C	NC
COM6017M	6	1	The Internet of Things	20	C	X
COM6018M	6	1	Penetration Testing and Vulnerability Assessment	20	C	X
Choose 40 credits from the following optional modules:						
COM6019M	6	2	Software & Web Security	20	O	X
COM6020M	6	2	Privacy & Data Protection	20	O	X
COM6021M	6	2	Network Security Architecture and Operations	20	O	X
COM6022M	6	2	Cloud Computing Security & Compliance	20	O	X
COM6023M	6	2	Advanced Web Development	20	O	X

Please note that not all options may be available every year as they depend on student demand and staff availability.

Any modules that must be passed for progression or award are indicated in the table above as non-compensatable. A non-compensatable module is one that must be passed at the relevant level (with a mark of 40) in order to progress.

Learning, teaching and assessment.

Level 4 gives you the fundamental core knowledge and understanding of essential facts, concepts, principles relating to computing and cyber security; providing you with a broad range of opportunities to develop core subject knowledge in the areas of programming for the web, mathematics, object-oriented programming, and the critical discourses surrounding developments in the field of cyber security. You will become familiar with common computer science terminology and well-versed in discipline-specific technical practices,

methodologies, and theories. Teaching at this level comprises a range of immersive learning experiences such as lectures, seminars, workshops, teaching laboratories, Supported Open Learning (SOL), guest talks, and trips.

Level 5 will enable you to further develop your subject knowledge through modules such as Information Security and Risk Management, Computer Networks, and Digital Forensics. You will undertake a Professional and Research Practices module allowing you to apply your skills in a 'live' setting, working for an established company or undertaking a self-initiated, possibly collaborative, entrepreneurial project or writing and acquiring professional certifications. This opportunity will enable you to apply and test the knowledge you have acquired so far through your degree and validate your skills needed to succeed across various Cyber Security careers.

Optional year in industry programme route

You will have the option of undertaking a year in industry (sandwich year), in between level 5 and level 6. Through this you will gain valuable experience in real employment. York St John University will provide you with support to help source a placement which meets your career aspirations, however it is your responsibility to secure your own placement. Support will be available through the CPD framework, and central University services such as the Careers and Employability Team. Students who undertake the year in industry often return for level 6 more focused on their studies and are deemed more job ready by employers. You will be prepared for your placement year through activities in semester two, level 5, which will assist you in making preparations for applying for and undertaking a placement. This will include CV and cover letter writing, as well as interview skills. You will work with the central University services with the support of an academic tutor to identify placement opportunities. On achieving a year in industry placement, you will complete a negotiated learning agreement in the form of a learning contract, which will be negotiated with your host firm and agreed by an academic from the York St John University Computer Science Team. This will be logged by the University, and you will be expected to demonstrate your achievement while on placement through a portfolio of evidence. In order to undertake a year in industry placement you will need to have achieved the minimum requirements for progression at level 5 and will also have to satisfy the following criteria:

- You must have passed all modules from level 4 and level 5.
- You must demonstrate a good level of professionalism in your academic conduct within the University, to the point where an academic from the computing team is willing to agree your suitability for the proposed placement.

During the year in industry placement, you will be allocated a mentor from within the University, who will monitor your progress throughout the placement. This may include Skype/email conversations. You will have a minimum of one field visit which will include a conversation with the employer.

Level 6 includes advanced modules in your field, allowing you to specialise and accent your learning via a choice of optional modules, for example: Penetration Testing and Vulnerability Assessment, Network Security Architecture and Operations, Privacy & Data Protection, Cloud Computing Security & Compliance, Privacy & Data Protection. Accompanying this you will undertake a Dissertation - a year-long independent research project of your own design, agreed by and supported by an academic supervisor. This project may be in any existing or emerging field of cyber security research and development. You are encouraged to consolidate technical learning and professional research interests through this Dissertation project. Teaching and learning at level 6 again incorporates the modes of delivery and activity encountered at levels 4 and 5, however, the emphasis at level 6 is on independent self-directed work that responds to learning within and across modules.

The teaching and learning environment of the programme is underpinned by a number of explicit pedagogic choices: small classes and small lab class sizes; so that you can get as much help when needed. Teaching and learning is based on a working with/co-creation rather than a teaching to approach – teaching has a strong practical element running through all modules within the degree.

Our approach to learning is holistic and practice focus. It will provide you a blend of theoretical and practical learning opportunities to enable you to apply practical and analytical skills synthesise information and ideas in an integrated way, so your learning experiences are authentic and relevant to your cyber security role.

Our approach to learning is cooperative. You will work solo and together in small groups with other students, building supportive relationships, reflecting on your experiences, and mentoring each other to achieve your full potential.

The assessment strategy for the programme focuses on your analytical skills, ability to integrate what you learn in real-world contexts and enables a wide range of skills to be assessed fairly and in multi-faceted manner. You will be solving real-life problems either in group or solo on projects that address global, social, political, and economic issues.

We use Technology Enhanced Learning to create a varied learning experience. Virtual Learning Environments provide you with opportunities to learn through online lectures, discussion groups, and online learning activities. You will be exposed to using virtualisation and cloud computing technologies and specialised cyber security hardware equipment for your practices. Online library resources specific to your subject guides, databases, and eBooks, and eJournals are easy to access and help support your study.

During your programme you will be asked to do 'formative' work that prepares you for assessment. This may be written or practical work. Formative work provides your academic assessors with opportunities to explore how you are doing and provides you with feedback to support your development. It also offers you the opportunity to review your progress, identify your strengths and areas of growth and ask for support where you think you need it. We may also ask you to provide feedback to the other students as part of reflective learning and coaching activities.

Progression and graduation requirements

The University's general regulations for undergraduate awards apply to this programme.

Any modules that must be passed for progression or award are indicated in the Programme Structure section as non-compensatable.

Late result modules
Indicate any module codes where the result of the first attempt is not known in time for the June School Assessment Panels (or equivalent level progression point for non-standard entry points).

COM5016M - Professional and Research Practices

Internal and external reference points

This programme specification was formulated with reference to:

- University mission and values
- University 2026 Strategy
- QAA Subject Benchmark for Computing (October 2019)
- Guidelines on course accreditation Information for universities and colleges (January 2020)

Date written: July 2021.