UNIVERSITY of BRADFORD

Faculty of Engineering and Informatics

Department of Computer Science

MSc Cyber Security Programme Specification

Academic Year	**2021/22**
Degree Awarding Body	**University of Bradford**
Final and interim awards at Level 7 FHEQ (Framework for Higher Education Qualifications)	**Degree of Master of Science** **Postgraduate Diploma** **Postgraduate Certificate**
Programme accredited by	**BCS The Chartered Institute for IT**
Programme admissions	**September and January**
Programme duration	**12 months full time,** **24 months part time**
QAA Subject benchmark statement	**Computing (2016),** **Master's Degrees (2010)**
Date last confirmed by Faculty Board	**January 2021**

Please note: This programme specification has been published in advance of the academic year to which it applies. Every effort has been made to ensure that the information is accurate at the time of publication, but changes may occur given the interval between publishing and commencement of teaching. Any change which impacts the terms and conditions of an applicant's offer will be communicated to them. Upon commencement of the programme, students will receive further detail about their course and any minor changes will be discussed and/or communicated at this point.

Introduction

Why Cyber Security?

The programme is designed to offer graduates the opportunity to develop a deeper understanding of cyber security as a discipline. The focus within MSc Cyber Security on the principles, technologies and practices of cyber security helps students to gain the appropriate skills for future PhD studies and research careers as well as to become competent practitioners. The key motivation for the current programme curriculum is to ensure that all graduates have studied relevant security disciplines that reflected the aims of the United Kingdom Government Communications Headquarters (GCHQ) National Security Programme whilst adhering to the curriculum framework within the University of Bradford. In effect, it is considered imperative that students will have an in-depth understanding of the issues faced by modern organisations.

This programme meets a continued growing demand for specialists in this area by offering individuals in current employment as well as recent graduates to enhance and develop their skills with advanced study of IT security, to equip them for senior positions with responsibility for the technical and security management of an organisation. The programme comprises particular developments in security with a firm base in academic research and also offers the opportunity for students to study selected topics in advanced

computer science, such as additional qualifications in Certified ISO/IEC 27001 Lead Implementer and CEH v10 Ethical Hacking.

A professional and industry-informed programme

Students with relevant industry skills are encouraged to specialise in cyber security or refine and develop their existing expertise.

Our teaching is informed by industry in several ways. Staff undertaking KTP projects, national and EU funded research projects and consultancy work embed new knowledge and concepts into their teaching materials and curriculum planning, based on the research and development work they conduct.

Students get exposure to industry throughout their programme as this is embedded in a number of ways. Throughout the academic year industrial speakers deliver invited talks that inform and inspire our students about current and future developments within their disciplines. In addition, industry qualifications such as ISO27001 Lead Implementer and CEH v10 Ethical Hacking are integral to the programme design.

Student societies with links to professional bodies afford further opportunities for our students to engage with industry, such as Pi Soc as the first ever BCS Student Chapter, and our ACM student chapter. These societies are encouraged and supported by the School to participate in industry led activities such as programming competitions, data dives and extra-curricular visits.

MSc Cyber Security at the University of Bradford

The Department of Computer Science has for many years successfully taught a range of programmes at undergraduate and postgraduate level. This programme draws upon the successful research expertise of the Department of Computer Science from within the Faculty of Engineering and Informatics in the University in addition to that within the Interdisciplinary Research Centre (IRC) in Cyber Security. This IRC has members from within Peace Studies, Engineering, Electrical Engineering, Computer Science, Mathematics, Telecommunications, Management, Law, Sociology and Psychology. This broad base of expertise and research is a fantastic resource for the continued development of the programme in cyber security.

The Cyber Security programme was originally introduced in 2004 and has run every year since then. The programme as a whole has been significantly revised to enhance its contents and ultimately the skills of all students graduating. This development process has taken a number of years and as such has included discussion and feedback from a number of academics, students, alumni, professionals and external examiners.

The main goal of this MSc Cyber Security programme is to prepare professionally trained graduates for industry. In this respect, detailed discussions have taken place, initially with industry professionals, who along with all other stakeholders have had a major input into shaping the revised programme.

Our Industry Advisory Board (IAB), with a membership comprised of industry representatives from both regional and national companies, meets twice a year to review our existing provision and to propose improvements to our courses. The programme includes the opportunity to enhance industry relevant skills with study in ISO27001 Lead

Implementer and Ethical Hacking. These skill areas were highlighted by past alumni and industry practitioners for inclusion in the programme.

Programme Aims

The MSc programme in Cyber Security is intended to respond to current academic challenges provided by increasing reliance on computers and networks for core business activity and to meet commercial needs for employees who are able to understand and think strategically about future developments in this area. The programme provides a high academic quality of service to students, covering both theoretical and practical aspects of computing, networking and cyber security. It enables students to equip themselves with knowledge, skills and understanding, at an advanced level within the chosen field of study.

On successful completion of the MSc Cyber Security students will have advanced knowledge of the principles and applications of network, computer and systems security through:

- **Systematic Understanding** and a critical awareness at advanced level, of core computing, networking and security subjects including security technologies, detailed understanding of the implications and issues relating to secure applications; recognition of the influence of the cyber world on secure system design and evaluation, and application development for firewalls, authentication, encryption, certificates and security protocols.
- **Discipline Specific Skills**, showing originality in the application of knowledge, together with a practical understanding of how established techniques of research and enquiry in security and cyber technologies are used to create and interpret knowledge in the discipline; the ability to design, implement, and evaluate secure systems; development of critical understanding of regulatory and practical issues relating to cyber security.
- **Personal and Transferable Skills** necessary for employment requiring: the exercise of initiative and personal responsibility; decision-making in complex and unpredictable situations; and the independent learning ability required for continuing professional development.

Admission Requirements

We take into consideration a number of factors when assessing your application. It's not just about your grades; we take the time to understand your personal circumstances and make decisions based on your potential to thrive at university and beyond.

The standard entry requirements for the programme are typically an undergraduate degree classified at 2:2 or above.

The University of Bradford has always welcomed applications from disabled students, and these will be considered on the same academic grounds as are applied to all applicants. If applicants have some form of disability, they may wish to contact the Disability Service before they apply at www.bradford.ac.uk/disability/before.

Please note: The information above relates to the contemporary recruitment cycle at time of publication and therefore may now be out of date. The current entry requirements are published online at www.bradford.ac.uk/courses/pg/cyber-security.

Recognition of Prior Learning

Applications are welcome from students with non-standard qualifications or mature students (those over 21 years of age on entry) with significant relevant experience.

If applicants have prior certificated learning or professional experience which may be equivalent to parts of this programme, the University has procedures to evaluate and recognise this learning in order to provide applicants with exemptions from specified modules or parts of the programme.

Intakes available

Students admitted to the programme in September study in the semester pattern of 1,2,3. Students admitted in January study in the semester pattern of 2,3,1. Part time routes are available for both admission periods. Students on part-time routes will study the taught component in year 1 and complete the dissertation in year 2.

Programme Learning Outcomes

To be eligible for the award of **Postgraduate Certificate** at FHEQ level 7, students will be able to:

1. Demonstrate an advanced understanding and application of some of the theories, principles and techniques applicable in the field of Cyber Security.
2. Demonstrate a systematic understanding and critical awareness of secure; systems within an organisation and the technical, legal and business issues involved.
3. Demonstrate a systematic understanding and critical awareness of the nature of a computer related crime and the people and organisations involved therein.
4. Demonstrate an advanced understanding of, and ability to apply concepts and principles underlying cryptographic primitives and protocols.
5. Demonstrate a comprehensive and critical understanding of techniques specific to the field of computer security.

Additionally, to be eligible for the award of **Postgraduate Diploma** at FHEQ level 7, students will be able to:

6. Critically analyse, model, construct and evaluate specific types of networks and be able to effectively implement a reliable and effective security protocol.
7. Select, adapt and apply the underlying technologies of secure systems.
8. Be proficient in the practical and theoretical concepts of computer science, current and emerging trends in technology.

Additionally, to be eligible for the award of **Degree of Master** at FHEQ level 7, students will be able to:

9. Select, design, plan and manage a self-directed and managed research-informed project.

10. Demonstrate a critical awareness of current and possible future opportunities and problems in; Internet, Computer and System Security evaluating current developments and trends.

Learning and Teaching Strategy

The programme includes innovative and active learning methods. Throughout the programme, we make use of case studies so that students can apply their theoretical understanding to real-world issues. In this way, abstract concepts are brought to life through practical activities. We also use methods associated with the "flipped classroom" where content is outside the classroom leaving more time and space for activities and active learning within tutorial and lecture sessions.

In addition to the standard technology enhanced learning approaches, we embed technologies to deliver key concepts in an interactive environment that strongly links theory with practical skills. For example, we link remotely with industry experts to deliver interactive sessions for developing student's pen-testing skills.

Research active staff are involved in curriculum development based on their research activities, exposing students to the very latest and future developments within their field of expertise. We integrate knowledge and experience from Industrial partners through both our Industry Advisory Board and research projects through case studies, lab-based activities and invited talks, ensuring that research findings are at the heart of our curriculum.

The programme offers a curriculum with core elements in Cyber Security. Dissertation work further enriches the opportunities students have to take control of their own learning. A range of teaching and learning methods is employed including lectures, tutorials, laboratory work and directed private study. Each 20-credit module on the programme requires students to commit 200 hours of study. Some of these hours will be formally timetabled - lectures, laboratories, seminars, tutorials and workshops whilst others will involve students carrying out private study.

Four workshop sessions act as a springboard for consideration and integration of Legal Social Ethical and Professional (LSEPI) issues into the project work from its commencement. All students progressing onto the dissertation are required to attend these workshops. As part of the workshop series, seminar sessions will take place to introduce the concepts and wider context of LSEPI practices within the Computing discipline (e.g. analysis skills, the research process, dissertation outlines and managing projects, data protection, computer misuse, ethics etc.). The seminars define relevant terms and the implications for professional practice within Computing. These are followed by a tutorial session with a case study scenario for groups of students, and the members of staff supervising dissertations, to discuss and debate the various aspects of LSEPI practice that would impact upon the scenario and the possible decisions and hypothetical outcomes. The tutorial concludes with a plenary to discuss the wide variety of issues and viewpoints from the groups and the implications for their dissertation work.

To ensure these topics are developed within a students' dissertation period, these initial workshops will be strengthened through the requirement for students to discuss these issues with their supervisor on a one-to-one basis. In addition, students will be required to

complete an Ethical Approval Form with the aim of highlighting any potential ethical and legal implications of the work proposed.

Assessment Strategy

Assessment for this programme is designed to develop skills in the area of cyber security in addition to more generic professional transferable skills such as team working, communication, leadership and decision making. The combination of group work, individual submissions, examinations, theoretical work and lab-based exercises helps develop skills that are essential in industry. Alongside gaining an MSc Cyber Security, students have the opportunity to gain additional qualifications in ISO/IEC 27001 Lead Implementer and CEH v10 Ethical Hacking if they undergo additional assessment.

All our staff have achieved, or are working towards, Fellowship of the Higher Education Academy. As part of our commitment to Excellence in Learning and Teaching, we conduct research into innovative and effective teaching methods. For example, assessment for projects was enhanced by incorporating regular formative and summative feedback opportunities to enhance the final outcomes.

Curriculum

The MSc Cyber Security covers a range of specialist topics, leading to the qualification of a Master's degree with the option to study for additional industry qualifications. Typically, a taught full-time Master's programme lasts for 12 months of full-time study (or 24 months part-time).

The relevance of the programme’s content to the stated teaching aims and objectives is based on core computer science and informatics topics as well as modules on relevant cyber security in relationship to secure implementation of systems, and their application in practice. Students will have opportunity to enhance Personal Transferable Skills principally through participation in and taking responsibility for a major individual project.

The programme has two stages: the taught programmes stage which takes place during the first two semesters (or four semesters for the part-time route), and the project/dissertation stage. The taught programmes stage is organised on a modular basis. All modules are classed as Core modules and are assessed at FHEQ Level 7.

The programme has modules in the Autumn and Spring periods providing grounding and advanced study of the field. The final two semesters allow students the opportunity to develop, through sustained major project work, advanced knowledge and understanding of cyber security.

The curriculum may change, subject to the University's programme approval, monitoring and review procedures.

Programme structure

Module Code	Module Title	Credits	Study Period
COS7030-B	ISO27000 Framework (ISMS)	20	Autumn (S1)
COS7024-B	Networks and Protocols	20	Autumn (S1)
COS7047-B	Advanced Cryptography	20	Autumn (S1)
COS7023-B	Internet Security and Protocols	20	Spring (S2)
COS7035-B	Business Systems Security	20	Spring (S2)
COS7029-B	Ethical Hacking	20	Spring (S2)
COS7004-E	Dissertation	60	Academic Year (S2+3)

Students will be eligible to exit with the award of **Postgraduate Certificate** if they have successfully completed 60 credits and achieved the award learning outcomes.

Students will be eligible to exit with the award of **Postgraduate Diploma** if they have successfully completed 120 credits and achieved the award learning outcomes.

Students will be eligible for the award of **Degree of Master** if they have successfully completed 180 credits and achieved the award learning outcomes.

Assessment Regulations

This Programme conforms to the standard University Postgraduate Assessment Regulations which are available at the following link: www.bradford.ac.uk/regulations

Minor Modification Schedule

Version Number	Brief description of Modification	Date of Approval (Faculty Board)
5	Updates for Academic Portfolio Review in February 2016	**December 2015**
6	Modification to curriculum structure	**March 2019**
7	Module COS7030-B moved from Sem 2 to Sem 1	**March 2020**
8	Specification reformatted and made accessible. Text updated to accommodate January intake.	**December 2020**
9	Annual changes for 2021 academic year	**June 2021**