Course Title	MSc Cyber Security
Final Award	MSc Cyber Security
Interim Awards	Postgraduate Diploma of Higher Education in Cyber Security Postgraduate Certificate of Higher Education in Cyber Security
Awarding Body	Ravensbourne University London
Teaching Institution	Ravensbourne University London
HECOS code (with Subject percentage Splits if applicable)	
QAA Subject Benchmark	Computing (Postgraduate) 2022
External Accrediting Bodies	N/A
Apprenticeship Standard used to inform the development of the course (if applicable)	N/A
Accelerated Degree Option	N/A
Study Load	☒ Full-time ☒ Part-time
Mode of study	☒ Face-to-face ☐ Blended ☐ Online
Delivery Location(s)	☒ Ravensbourne University campus ☐ Online
Length(s) of Course(s)	1 year full time 2 years part time
Type (open/closed)	Open
Validation period	5 Years (September 2022 – September 2027)
Intended First Cohort Start Date	September 2022
Date produced/amended	June 2022
Course Leader	TBC
Course Development Team Members	Ajaz Ali
Course Administrative Contact	Charles Mullany

Course Description

Ravensbourne has an established international reputation for innovation at the intersection of design and digital media. The proposed suite of MSc programmes – of which the MSc Cyber Security course is an integral part – seeks to capitalise on and consolidate these successes, expanding Ravensbourne's activities from its current position as innovative user of technologies to innovative creator of technologies. The course invites prospective postgraduate students to be part of that journey, empowering them to draw on and learn from this rich history of innovative design thinking and apply this to the creation of new technologies.

To facilitate this, the MSc Cyber Security course is targeted at graduates and professionals who already have a background in Computer Science, Computer Networking or a related field and who are seeking to update and consolidate their existing technical knowledge through rigorous study of Cyber Security. To this end, the course offers modules in a range of cutting-edge areas including: Systems Architecture, Network Security, Cyber Incident Response, Cyber Forensics and Open-Source Intelligence. In covering these subjects, the curriculum helps students gain core skills for cyber incident protection, response and investigation. It also provides knowledge for designing cyber secure systems.

A significant benefit of Masters level study is the expansion of students' professional network. In recognition of this and in anticipation of the benefits that arise from it, MSc Cyber Security shares the three core non-technical modules with its sister programmes MSc Computer Science, MSc Artificial Intelligence. In sharing these modules, the curriculum seeks to facilitate peer-to-peer learning and collaboration between students with differing knowledge and expertise.

Semester 1

In Semester one, MSc Cyber Security students will undertake two technical modules in 'Computer and Network Security' (CNS) and 'Hacking and Incident Management' (HIM). Each module will give students core knowledge in a different area of cyber security. The CNS module will ensure students have a good understanding of the fundamentals of the subject and technical aspects of securing and managing computer networks.

Students will undertake "introduction to Research" unit which is aa combined unit with other computing courses, providing a much needed option for interaction

Semester 2

In Semester two, students will undertake "Secure Systems and Open Source Intelligence" and "Digital Forensics and Cyber Crime". Cyber Incident Management is a highly desirable professional skill which aligns to the ISO 27001 standard. As such, it has significant import and effects into the business domain. This combination of modules provides an excellent opportunity for students to explore how business processes interact with formal processes, for cyber defence and response. Alongside this, students begin their dissertation module in this semester, which will run until the end of Semester 3. The dissertation module will introduce students to postgraduate level scientific research methodologies and invite them to design and execute a non-trivial piece of cyber security focused research.

These modules will introduce students to a synergy of technical and analytical skills. In Cyber Forensics they will learn the fundamentals of carrying out a cyber forensic investigation. This will include technical processes such as disk imaging and static image analysis; and will also include important aspects like maintaining evidence integrity in a chain of custody, via practices such as hashing. Through this study, students will learn how to conduct an effective cyber forensic investigation. In Open-Source Intelligence, students will learn cutting edge techniques for identifying and/or tracking individuals and/or organisations, through internet-focused investigations.

Semester 3

One key feature of this semester is “Negotiated Practice” unit which provides support in development of ideas for Final Major Project, various research techniques and development of a realistic plan to achieve the final outcome of this course in semester 3 where they will focus on Final Project only.

Overall, the course provides students with an excellent opportunity to improve their cyber skillset, expand their knowledge and deepen their understanding of how Cyber Security skills may be applied to secure systems, defend networks and investigate cyber incidents when defences fail.

In summary, the distinctive features of the course includes:

1. Learning focused on the prevalent cutting-edge areas of Cyber Security
2. Professional networking opportunities with postgraduate students from other disciplines
3. Practical curriculum, geared towards the application of Cyber Security to business, technical and civic domains
4. Study into Open-Source Intelligence techniques. This is not a widely offered topic within typical university cyber programmes - a distinctive USP for this comprehensive MSc curriculum.

Course Aims

- To produce graduates who can apply Cyber Security skills and knowledge to secure and protect real-world systems
- To improve student understanding of the impact of engineering decisions across a broad range of spectrums
- To support and encourage the development of an innovation mindset
- To enable students to identify professional development goals that will lead them into future career opportunities
- To support students in developing a professional network via interactions with peers, tutors and other professionals, that may provide future value and support to them as their career develops
- To encourage students to understand and embrace the concept of becoming a lifelong learner

Course Learning Outcomes

The course provides opportunities for students to develop and demonstrate knowledge and understanding, qualities, skills and other attributes in the following areas.

On completion of the **MSc Cyber Security** students will be able to:

Explore	Critically apply tools and technical skills to identify, model, and engineer systems and use established concepts and techniques from the study of Cyber Security to propose and analyse solutions to a range of security challenges.
Create	Solve a range of current and emerging cyber security challenges, demonstrating critical selection, evaluation and application of required tools and techniques.

	Select and apply engineering processes to comply with the legal and ethical considerations governing the use of computers and the processing of information to develop solutions which address real-world challenges.
Influence	Evaluate, refine, and apply comprehensive analytical and technical skills to solving a significant Cyber Security related challenge.
Integrate	Define a significant Cyber Security challenge, and professionally manage a process of work to propose and execute a viable solution to it using a recognised project management strategy.

On completion of the **Postgraduate Diploma of Higher Education in Cyber Security** Students will be able to:	
Explore	Apply tools and technical skills to identify, model, and engineer systems and use established concepts and techniques from the study of Cyber Security to propose and analyse solutions to a range of security challenges.
Create	Solve a range of current and emerging cyber security challenges, demonstrating critical selection, evaluation and application of required tools and techniques.
Influence	Evaluate, refine, and apply comprehensive analytical and technical skills to solving a significant Cyber Security related challenge.
Integrate	Define a Cyber Security challenge, and professionally manage a process of work to propose and execute a viable solution to it.

Where a student does not complete the full course, but exits with a Postgraduate Certificate, they will have had the opportunity to develop and demonstrate knowledge and understanding, qualities, skills and other attributes in the following areas. On completion of the **Postgraduate Certificate of Higher Education in Cyber Security** Students will be able to:	
Explore	Use established concepts and techniques from the study of Cyber Security to propose and analyse solutions to a range of security challenges.
Create	Explain a range of current and emerging cyber security challenges, demonstrating critical selection, evaluation and application of software engineering tools and techniques.
Influence	Evaluate comprehensive analytical and technical skills to solving a significant Cyber Security related challenge.
Integrate	Define a Cyber Security challenge, and professionally manage a process of work to propose and execute a viable solution.

Ravensbourne University Assessment Criteria	
Explore	Research and Analysis Subject Knowledge Critical Thinking and Reflection Problem Solving
Create	Ideation Experimentation Technical Competence Communication and Presentation
Influence	Social Impact Ethical Impact Environmental Impact
Integrate	Collaboration Entrepreneurship and Enterprise Professional Development

Core Competencies
Each module learning outcome should be aligned to at least one competency.

Competency	Definition	Aligned Assessment Criteria
Cognitive	The ability to acquire, retain and use knowledge, recognise, pose and solve problems. Attributes may include: • Evaluate their own beliefs, biases and assumptions • Evaluate strengths, weaknesses, and fallacies of logic in arguments and information • Apply lesson from the past or learned knowledge and skills to new and varied situations • Perform basic computations or approach practical problems by choosing appropriately from a variety of mathematical techniques • Devise and defend a logical hypothesis to explain observed phenomenon • Recognise a problem and devise and implement a plan of action	**Explore, Create, Integrate, Influence**
Creative	The ability to generate new ideas, express themselves creatively, innovate and/ or solve complex problems in an original way.	**Create**
Professional	The ability to understand and effectively meet the expectations of industry partners, through outputs and behaviours.	**Integrate, Influence**
Emotional, Social and Physical	Emotional -The intrapersonal ability to identify, assess, and regulate one's own emotions and moods; to discriminate among them and to use this information to guide one's thinking and actions and where one has to make	**Explore, Influence, Integrate**

	consequential decisions for oneself. Attributes may include:	
	• Self-awareness & regulation (including metacognition) • Mindfulness • Cognitive flexibility • Emotional resilience • Motivation • Ethical decision- making	
	Social - The interpersonal ability to identify & understand the underlying emotions of individuals and groups, enhancing communication efficacy, empathy and influence. Attributes may include:	
	• Managing your audience • Coordinating with others • Negotiation • Creativity • People management • Leadership & entrepreneurship • Service orientation • Active listening • Coaching and mentoring	
	Physical - The ability to perceive and optimise physiological activity and responses to influence emotion, solve problems or otherwise effect behaviour. Physical intelligence engages the body to train neuron pathways to help change an inappropriate response to an appropriate response. Attributes may include	
	• Self-discipline & management • Attention • Reaction & response time • Cognitive & muscle memory • Managing stress • Physical resilience	
Cultural		**Influence, Integrate**

	The capability to relate to and work effectively across cultures including intercultural engagement, cultural understanding and intercultural communication.	
Enterprise and Entrepreneurial	The generation and application of ideas within a practical setting. It combines creativity, idea generation and design thinking, with problem identification, problem solving, and innovation followed by practical action. This can, but does not exclusively, lead to venture creation (UK Quality Assurance Agency, Enterprise and Entrepreneurship Education 2018).	**Create, Influence, Integrate**
Digital	The confident adoption of applications, new devices, software and services and the ability to stay up to date with ICT as it evolves. The ability to deal with failures and problems of ICT and to design and implement solutions (Jisc Digital Capabilities Framework)	**Explore, Create, Integrate, Influence**
Ravensbourne Return	Engagement with inhouse activities including mentoring other students, volunteering, acting as a student rep or ambassador. Demonstrate a knowledge of current events and social issues Identify their personal convictions and explore options for putting these convictions into practice Engagement with the external community through (from) employment, volunteering, participation in a Professional Life or other programme-based project.	**Explore, Create, Influence, Integrate,**

Learning, Teaching and Assessment

Learning and Teaching methods	Assessment Strategy
Formal learning and teaching methods applied on this programme will predominantly take the form of: • Lectures • Practical Labs • Seminars • Research Projects • Tutorials (Group and Individual) These methods will be applied across the course in keeping with wider established practices in the field of Cyber Security education. Other methods may be applied as curricular enhancements, as deemed	An appropriate range of assessment methods will be used to support students across the course. Portfolios are used for several assessment processes. In the context of Cyber Security, these will normally consist of evidence of completed practical work and may optionally include some form of written report. For example, a piece of working software (practical) may be accompanied by formal software documentation (written). Portfolios are selected in the first instance for summative assessment since they may be

appropriate by the delivery team. These may include: • Flipped classroom activities • Live industry projects and/or briefs • Guest speaker talks • Visits to companies • Hackathons	assessed holistically. Students' marks are derived from the cumulative relationship between the study elements, rather than based on each single assessed element considered in isolation. Formative assessment techniques will also be used to monitor student learning and provide constant feedback for staff and students. This methodology gives the lecturer the optimum opportunity to mark to feedback and encourage, providing meaningful support and guidance to help the student develop to their full potential. Aside from portfolios, other common assessment strategies will predominantly include: • Reports • Presentations • Engineering Projects Summative and Formative assessment will be given in line with university regulations. Within Cyber Security, formative assessment will play a key part in helping students orientate and calibrate their skills. This may take place through individual and group class-based exercises and through activities in the Virtual Learning Environment (VLE). For example, lecturers may present tests and quizzes in the VLE that allow students to undertake simple exercises to test their memory and understanding of material covered in class.

Course Structure

Module Code	Module Title	Shared Module	Mandatory / Elective	Credits
Level 7				
MCY22701	**Computer Network and Security**	N	Mandatory	20
MCY22702	**Hacking and Incident Management**	N	Mandatory	20
MCY22703	**Introduction to Research**	Y	Mandatory	20
MCY22704	**Secure Systems and Open-Source Intelligence**	N	Mandatory	20
MCY22705	**Digital Forensics and Cyber Crime**	N	Mandatory	20
MCY22706	**Negotiated Practice**	Y	Mandatory	20
MCY22707	**Final Project**	Y	Mandatory	60
				180

Learning Hours

Learning Hours (per 20 credits)			
Staff – Student Contact Hours		**Independent Study Hours**	
Taught hours	36	Independent study, self-directed study and assessment	164
Total			200

Course Regulations

Entry Requirements
First, Upper Second Class or a 2:2 honours degree (or equivalent non-UK qualifications) in a relevant subject, or an equivalent professional qualification in a related subject area. If you are applying directly from an undergraduate degree course without experience or professional practice you must be able to demonstrate a good knowledge of your chosen subject area. Substantial professional work experience with relevant references could be considered for entry into this course. *Please refer to the institutional regulations on the expected minimum entry requirements (found under Section 5 of the General Academic Regulations found on the website here), and the course page on the Ravensbourne University website for course specific entry requirements.*
Accreditation of Prior Learning (if applicable)
Applications are welcomed from those who may not possess formal entry qualifications, mature students, those with work experience or with qualifications other than those listed above. Such applicants should demonstrate sufficient aptitude and potential to complete the course

successfully. Applicants will be assessed at interview in accordance with Ravensbourne’s Accreditation of Prior Learning Policy and Procedure.

Conditions for Progression

Students will be deemed to have passed a module if they achieve 40% for undergraduate students; or 50% for postgraduate students.

A student who has passed all assessments to date but has not yet reached the end of a level (or stage) will be permitted to proceed into the following semester by the Interim Assessment Board.

Reassessment of Failed Elements

Failure in any component will result in a Fail grade for the component.

Non-submission in any component will result in a non-submission for the component.

Students must then successfully retrieve the failed or non-submitted component by resubmission of assessment in order to pass the module.

Where a student does successfully retrieve a component failure, the grade for the component will be capped at 40% (undergraduate) or 50% (postgraduate) (except where Extenuating Circumstances have been approved). The overall grade for the module will be calculated using all achieved grades where there are 2 or more components.

Conditions for the Granting of Awards

A student who completes an approved course of study, shall be awarded Master of Science in Cyber Security.

Those students who exit the course without completing it may be entitled to exit with an award of either a:

1. Postgraduate Diploma of Higher Education in Cyber Security, provided they complete an approved course of modules and the learning outcomes for such award as set out in the Course Specification.
2. Postgraduate Certificate of Higher Education in Cyber Security, provided they complete an approved course of modules and the learning outcomes for such award as set out in the Course Specification.

Any derogation(s) from the Regulations required?

No

Student Support	https://www.ravensbourne.ac.uk/student-services
Assessment Regulations	https://www.ravensbourne.ac.uk/staff-and-student-policies

Learning Outcomes Mapping

Level 7							
Course LOs	Module 1	Module 2	Module 3	Module 4	Module 5	Module 6	Module 7
LO 1	X	X	X	X	X	X	X
LO 2	X	X	X		X		X
LO 3		X		X	X		X
LO 4	X	X		X			X
LO 5			X			X	X
LO 6	X	X		X		X	X

Course Diagram

Semester 1	Semester 2	Semester 3
MCY22701 Computer and Network Security 20 credits	**MCY22704 Secure Systems and Open Source Intelligence** 20 credits	**MCY22707 Final Project** 60 credits (shared)
MCY22702 Hacking and Incident Management 20 credits	**MCY22705 Digital Forensics and Cyber Crime** 20 credits	
MCY22703 Introduction to Research 20 credits (Shared)	**MCY22706 Negotiated Practice** 20 credits (Shared)	