MSc Cyber Security

Awarding institution	Bath Spa University
Teaching institution	Bath Spa University
School	Bath School of Design
Department	Creative Computing
Main campus	Newton Park
Other sites of delivery	Future Education World
Other Schools involved in delivery	N/A
Name of award(s)	MSc Cyber Security
Qualification (final award)	MSc
Intermediate awards available	PgCert, PgDip
Routes available	Single
Duration of award	1 year full-time, 2 years part-time
Sandwich period	No
Modes of delivery offered	campus-based
Regulatory Scheme[1]	Taught Postgraduate Framework

Professional, Statutory and Regulatory Body accreditation	N/A
Date of most recent PSRB approval (month and year)	N/A
Renewal of PSRB approval due (month and year)	N/A
UCAS code	N/A
Route code (SITS)	MSCS
Relevant QAA Subject Benchmark Statements (including date of publication)	Computing, Masters (2019)
Date of most recent approval	June 2020
Date specification last updated	February 2024

[1]This should also be read in conjunction with the University's Qualifications Framework

Programme Overview

This MSc programme focuses on meeting the challenges of cyber security faced by information assurance professionals working at the strategic and operational level. It covers the skills and knowledge needed by public and private sector executives to develop, monitor and evaluate cost-effective cyber risk management procedures. Across the course you learn digital-era leadership techniques and concepts, and develop the holistic understanding and analytical mindset necessary to deliver business benefits in a cyber-digital world. The curriculum offers an opportunity to upskill to leadership roles for current professionals, while offering graduates the critical insights needed to establish themselves in the ever-evolving field of cyber security.

Module content within MSc Cyber Security targets the following themes:

- Law and regulation
- Governance
- Asset evaluation
- Vulnerabilities
- Attack vectors
- Operational resilience
- Risk management
- Strategic planning

Programme Aims

1. Knowledge – to support a systematic understanding of cyber security as a field of study and how it interfaces with other parts of the computer industry.
2. Critical Thinking – to develop students who can critically assess potential threat actors and balance risk management strategies against business needs.
3. Research – develop the research capacity of students to advance their understanding of the rapidly evolving threat landscape, and how to develop effective responses that utilise emerging technologies.
4. Practice – to assist students in developing and maintaining efficient and comprehensive risk management strategies to meet the cyber security and operational resilience challenges of the future.
5. Employability – to elevate employability prospects within the digital economy by focusing on holistic perspectives, applied contexts, and effective leadership within the field of cyber security.

Programme Intended Learning Outcomes (ILOs)

(NB These ILOs are at level 7 of the FHEQ)

A Subject-specific Skills and Knowledge

A1 Environment – demonstrate critical awareness of current and emerging threat landscapes at both an organisational and national level, and the interactions of key professional roles that serve to address them.

A2 Information Security - evidence systematic knowledge of the theories, controls, and legal and regulatory frameworks that underpin an organisation's ability to protect the confidentiality, availability and integrity of its assets.

A3 Information Risk Management - demonstrate a comprehensive understanding of the policies, assessment tools and assurance methodologies used to identify, quantity and mitigate vulnerabilities related to information security.

A4 Operational Security - informed by critical evaluation and adaptation of current practice, evidence an ability to formulate security architectures and organisational procedures that maintain the protection of an IT estate and its stakeholders.

A5 Incident Management - devise strategies for real-time and post incident cyber incident analysis, investigation and active response that drive business continuity, recovery and future planning.

A6 Change Management and Policy Development - evidence a systematic understanding of the key levers, tools, techniques and metrics used to embed cyber security in digital transformation programmes.

B Cognitive and Intellectual Skills

B1 Critical Thinking – evaluate and synthesise complete and incomplete information from a range of sources to identify and analyse abstract problems or scenarios in the context of cyber security.

B2 Research – utilise established methods of research and enquiry to interpret and generate knowledge in the field of cyber security.

B3 Leadership - demonstrate a systematic approach to team management, communications, and delivering change and innovation in the field of cyber security.

C Skills for Life and Work

On achieving Level 7 you will be able to:

C1 Work Independently - Act autonomously in planning and implementing tasks in a professional context.

C2 Work with Others - Plan for and actively engage in inclusive collaboration with others to tackle and solve complex problems and develop original insights.

C3 Communicate with Impact - Communicate complex ideas clearly, effectively and impactfully with specialist and non-specialist audiences.

C4 Demonstrate Digital Fluency - Use digital skills productively, critically and ethnically to enhance creativity and communication in a professional context.

Intermediate awards

PgCert Intended Learning Outcomes
A1, A2, A4, A5, B1, B3, C1, C2, C3, C4

PgDip Intended Learning Outcomes
A1, A2, A3, A4, A5, A6, B1, B3, C1, C2, C3, C4

Programme content

This programme comprises the following modules

Key:

Core = C

Required = R

Required* = R*

Optional = O

Not available for this status = N/A

If a particular status is greyed out, it is not offered for this programme.

MSc Cyber Security				Status	
Level	Code	Title	Credits	Single	Joint
7	CYS7000-30	Cyber Security Bootcamp	30	C	
7	CYS7001-30	Business Security Architecture	30	C	
7	CYS7002-15	Critical Vulnerability Analysis	15	C	
7	CYS7003-15	Offensive and Defensive Cyber Operations	15	C	
7	CYS7004-15	Critical National Infrastructure	15	C	
7	CYS7005-15	Cyber War	15	C	
7	CYS7006-60	Dissertation	60	C	

Assessment methods

A range of summative assessment tasks will be used to test the Intended Learning Outcomes in each module. These are indicated in the attached assessment map which shows which tasks are used in which modules.

Students will be supported in their development towards summative assessment by appropriate formative exercises.

Work experience and placement opportunities

There are several opportunities to engage with industry across the programme. We encourage you to take advantage of:

- Guest lectures by practitioners with extensive and ongoing experience in the field.
- Opportunities to attend local cyber security networking events e.g. Cyber Cluster, BCS.
- Graduate employment opportunities offered by local firms.
- Industry-insight visits to cyber training and operational facilities.

Additional Costs Table

There are no additional costs associated with this course.

Module Code & Title	**Type of Cost**	**Cost**

Graduate Attributes

	Bath Spa Graduates…	In MSc Cybersecurity, we enable this…
1	Will be employable: equipped with the skills necessary to flourish in the global workplace, able to work in and lead teams	Offering opportunities to interact with the cyber ecosystem in order to gain insights into leading edge approaches and methodologies
2	Will be able to understand and manage complexity, diversity and change	Enhancing research, critical thinking, problem scoping and team leadership skills to generate comprehensive responses to complex situations.
3	Will be creative: able to innovate and to solve problems by working across disciplines as professional or artistic practitioners	Through a series of conceptual, practical and application activities, the course will drive cross discipline understanding in delivering innovative solutions.
4	Will be digitally literate: able to work at the interface of creativity and technology	Working with a variety of industry-standard tools and technologies.

5	Will be internationally networked: either by studying abroad for part of the their programme, or studying alongside students from overseas	Sharing best practice though international cyber security expertise of the delivery team.
6	Will be creative thinkers, doers and makers	The structure of the course in terms of its concept, application and practical exercises encourages all students to explore creative problem solving approaches.
7	Will be critical thinkers: able to express their ideas in written and oral form, and possessing information literacy	Sharing techniques and best practices that help lead to accurate and probing reflective reports, participation in tabletop exercises representing pressurised business environments, C-suite briefs and research papers.
8	Will be ethically aware: prepared for citizenship in a local, national and global context	The comprehensive nature of the ecosystem will lend itself to ethical awareness and enterprise/ national consideration of the values of digital citizenship in personal and work settings

Modifications

Module-level modifications

Code	Title	Nature of modification	Date(s) of approval and approving bodies	Date modification comes into effect
All modules		updated to align with assessment policy	education committee June 2021	2021/22

Programme-level modifications

Nature of modification	Date(s) of approval and approving bodies	Date modification comes into effect

Attached as appendices:

1. Programme structure diagram
2. Map of module outcomes to level/programme outcomes
3. Assessment map
4. Module descriptors

Appendix 1: Programme Structure Diagram – MSc Cyber Security

Level 7 FULL TIME		
Trimester 1	**Trimester 2**	**Trimester 3**
Core Modules		
CYS7000-30 Cyber Security Bootcamp CYS7001-30 Business Security Architecture	CYS7002-15 Critical Vulnerability Analysis CYS7003-15 Offensive and Defensive Cyber Operations CYS7004-15 Critical National Infrastructure CYS7005-15 Cyber War	CYS7006-60 Dissertation

Level 7 PART TIME		
Year 1		
Trimester 1	**Trimester 2**	**Trimester 3**
Core Modules		
CYS7000-30 Cyber Security Bootcamp	CYS7002-15 Critical Vulnerability Analysis CYS7003-15 Offensive and Defensive Cyber Operations	CYS7006-60 Dissertation
Level 7 PART TIME		
Year 2		
Trimester 1	**Trimester 2**	**Trimester 3**
Core Modules		

CYS7001-30 Business Security Architecture	CYS7004-15 Critical National Infrastructure CYS7005-15 Cyber War	CYS7006-60 Dissertation

Appendix 2: Map of Intended Learning Outcomes

Level	Module Code	Module Title	Status (C,R,R*,O)	Intended Learning Outcomes												
				Subject-specific Skills and Knowledge						Cognitive and Intellectual Skills			Skills for Life and Work			
				A1	A2	A3	A4	A5	A6	B1	B2	B3	C1	C2	C3	C4
7	CYS7000-30	Cyber Security Bootcamp	C	X	X			X		X			X		X	X
7	CYS7001-30	Business Security Architecture	C	X	X		X		X	X		X	X	X	X	
7	CYS7002-15	Critical Vulnerability Analysis	C			X	X	X		X			X	X	X	X
7	CYS7003-15	Offensive and Defensive Cyber Operations	C	X		X	X	X		X		X	X	X	X	X
7	CYS7004-15	Critical National Infrastructure	C	X	X		X			X			X		X	
7	CYS7005-15	Cyber War	C	X	X	X		X		X		X	X	X	X	X
7	CYS7006-60	Dissertation	C	X	X	X	X	X	X	X	X		X	X		

[4] C = Core; R = Required; R* = Required*; O = Optional

Appendix 3: Map of Summative Assessment Tasks by Module

Level	Module Code	Module Title	Status (C,R,R*,O)[1]	Assessment method													
				Coursework						Practical					Written Examination		
				Composition	Dissertation	Essay	Journal	Portfolio	Report	Performance	Practical Project	Practical skills	Presentation	Set exercises	Written Examination	In-class test (seen)	In-class test (unseen)
7	CYS7000-30	Cyber Security Bootcamp	C			1x (5000 words)			1x (3000 words)								
7	CYS7001-30	Business Security Architecture	C						1x (5500 words)			1x					
7	CYS7002-15	Critical Vulnerability Analysis	C						1x								

7	CYS7003-15	Offensive and Defensive Cyber Operations	C				1x (2000 words)				1x (4000 words)						
7	CYS7004-15	Critical National Infrastructure	C								1x		1x				
7	CYS7005-15	Cyber War	C						1x				1x				
7	CYS7006-60	Dissertation	C		1x (14000 words)								1x				

[1] C = Core; R = Required; R* = Required*; O = Optional