BSc (Hons) Cyber Security

Contents

Overview

Awarding institution	Bath Spa University
Teaching institution	Bath Spa University
School	Bath School of Design
Department	Cyber Security
Main campus	Newton Park
Other sites of delivery	Future Education World
Other Schools involved in delivery	n/a
Name of award(s)	Cyber Security
Qualification (final award)	BSc (Hons)
Intermediate awards available	Diploma of Higher Education Certificate of Higher Education
Routes available	Single Honours
Sandwich year	Yes
Duration of award	3 years full-time (4 years with Professional Placement Year) 6 years part time
Modes of delivery offered	Campus-based
Regulatory Scheme[1]	Undergraduate Academic Framework
Exemptions from regulations/framework[2]	n/a
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	CS01 CS02 (with professional placement year)
Route code (SITS)	CYSSIN CYSSIN (with professional placement year)
Relevant QAA Subject Benchmark Statements (including date of publication)	Computing (October 2019)
Date of most recent approval	June 2023
Date specification last updated	April 2024

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

[2] See section on ‘Exemptions’

Exemptions

There are no exemptions.

Programme Overview

BSc (Hons) Cyber Security prepares you to meet the evolving challenges of protecting the digital systems and services we rely on in daily life, as well as responding effectively to instances where their vulnerabilities are exploited by threat actors. You learn through a blend of theory and practical work that cuts across knowledge in computing and cyber security, that engages tools and techniques employed in industry, and is supported by interaction with real-world business scenarios. Across the course you are exposed to many aspects of cyber security, from key professional roles and their remits, through network design and administration, to the nuances of establishing robust strategies for organisational cyber resilience. The aim of BSc (Hons) Cyber Security is to support a holistic understanding of the subject, therefore facilitating access to a wide range of professional careers in the field.

Module content targets the following themes:

- Software development
- Analytical thinking
- Problem solving
- Network design and administration
- Intrusion detection and response
- Digital forensics
- Offensive and defensive cyber operations
- Cyber resilience
- Governance, risk and compliance

Themes are engaged via a learning path that establishes core computing skills in year 1, expands your understanding into specialist areas of cyber security in year 2, and broadens in year 3 to support greater awareness of the context in which cyber security issues permeate society. Through a range of learning activities and applied teaching methods, you gain a balanced apprehension of the systems under threat, and practical knowledge of the tools, frameworks and procedures that assist their defence.

Year 1 introduces the fundamental concepts and skills that underpin computing and cyber security, including programming, system design and development, and digital forensics.

Year 2 builds on the computing theme with an increased emphasis on the security concepts, tools and techniques that are deployed to protect digital systems. Modules cover practical security considerations such as defense through secure network design, intrusion detection, and strategies for enhancing organisational cyber resilience.

Year 3 comprises specialist modules that deepen your understanding of the challenges and operational practices of cyber security. Modules include those that examine vulnerability assessment methodologies such as red teaming, strategies for protecting critical national infrastructure, and the law, regulations and ethical concerns that underpin the field.

Programme Aims

1. Knowledge – to support an applied understanding of critical concepts, principles and practices within the field of cyber security.
2. Context - to cultivate a deep appreciation of the relevance of cyber security in society and improve the understanding of secure design and secure development in the computer industry.
3. Computational Thinking – to develop individuals that have a capacity to analyse complex cyber security problems and propose holistic solutions that rely on the application of computing, and that are informed by human, technical and process considerations.
4. Critical Thinking – to develop students that can critically evaluate cyber security knowledge in wider context and apply it in personal, business and public sector contexts.
5. Practice – to assist students in establishing and maintaining risk assessment and management strategies that meet a range of cyber security and critical vulnerability challenges.
6. Ethics - to outline the complexities of ethical practice in cyber security, and encourage students to reflect critically on the human consequences of their practices, behaviours and approaches to decision-making in the field.
7. Employability – to embed industry-insight and professional development opportunities across the programme to ensure that students are prepared for roles in the cyber security sector.

Programme Intended Learning Outcomes (ILOs)

A Subject-Specific Skills and Knowledge

	Programme Intended Learning Outcomes (ILOs) **On Achieving Level 6**	**On Achieving Level 5**	**On Achieving Level 4**
A1	Sector Context – Systematic understanding of current developments in the cyber security sector, and the ability to identify and critically evaluate emerging challenges, practices and technologies in the field.	Sector Context – An applied understanding, and ability to critically evaluate, the operational mandate of a specialist role within the cyber security sector.	Sector Context – Knowledge of the core objectives of the cyber security sector and its key professional roles.
A2	Law, Regulation and Ethics - Systematic understanding of cyber security law and regulation, and the ability to critically examine the legal and ethical implications of decisions in cyber security, including instances that present moral conflict.	Law, Regulation and Ethics - the ability to critically evaluate the legal and regulatory underpinnings and ethical dimension of key professional roles in the field of cyber security.	Law, Regulation and Ethics - Knowledge of key laws, regulation and ethical concerns in the field of cyber security.
A3	Systems – The ability to systematically evaluate business security architectures and their component systems to identify potential vulnerabilities and propose modifications that enhance cyber resilience.	Systems – An applied understanding of the design and implementation methods of computing and cyber security systems.	Systems – Knowledge of the key functions, features and design considerations of computing and cyber security systems.
A4	Tools – The ability to critically evaluate, select and deploy in a systematic manner specialist tools as required to address a problem in the field of cyber security.	Tools – The ability to critically evaluate and apply established computing and cyber security tools.	Tools – Knowledge of the function, benefits and limitations of core computing and cyber security tools.
A5	Threat Analysis - Systematic knowledge and the ability to critically evaluate current and emerging threat vectors and their associated threat actor motivators and geopolitical factors.	Threat Analysis - The ability to critically evaluate and apply sector-standard methods of detecting and analyising a range of threat vectors.	Threat Analysis - Knowledge of routine threat vectors, the core objectives of threat actors, and the human factors that contribute to data breaches.
A6	Incident handling - The ability to critically evaluate, implement and adapt specialist methodologies in the field of cyber security for preventive action and post-incident response.	Incident handling - The ability to critically evaluate and apply sector-standard methods of responding and recovering from network intrusions.	Incident handling - Knowledge of the core objectives and investigative procedures of digital forensics.
A7	Reporting - The ability to select, critically evaluate, implement and adapt strategies for reporting the outcomes of a specialist task in the field of cyber security.	Reporting - The ability to critically evaluate and apply established and evidence-based approaches to reporting the outcome of a routine task in the field of cyber security.	Reporting - Knowledge of key methods of reporting the outcomes of a computing task.

B Cognitive and Intellectual Skills

	Programme Intended Learning Outcomes (ILOs) **On Achieving Level 6**	**On Achieving Level 5**	**On Achieving Level 4**
B1	Knowledge – Systematic knowledge of, and the ability to critically evaluate established and emerging concepts, practices and terms in the field of cyber security.	Knowledge – Critical understanding of established concepts, principles and terms in the field of cyber security.	Knowledge – Knowledge of the fundamental concepts, principles and terms that underpin the field of cyber security.
B2	Computational Thinking – The ability to critically evaluate and apply methods of deconstructing abstract problems and proposing solutions that are efficient and generalisable.	Computational Thinking – The ability to apply established frameworks for computational thinking to represent a complex problem appropriately and reduce it to a series of ordered, solvable steps.	Computational Thinking – The ability to express a defined problem as a series of small and solvable steps.
B3	Critical Thinking – The ability to collect, analyse, generate where required, and synthesise sources of information and data in order to address an abstract problem in the field of cyber security.	Critical Thinking – The ability to identify sources of information and data that are relevant to a particular problem domain, then critically evaluate and apply methods of analysis to generate insights.	Critical Thinking – Knowledge of key methods used in computing and cyber security to analyse and extract insights from a source of information.

B4	Collaboration - A systematic understanding of collaborative strategies in the field of cyber security and its value in diversifying expertise, enhancing real-time visibility and cultivating cross-sector relationships.	Collaboration - Critical understanding of, and the ability to apply, collaborative practice to address challenges in the field of cyber security.	Collaboration - Awareness of key methods of collaboration in the field of cyber security, and the rationale for sharing information between stakeholders.

C Skills for Life and Work

	On achieving Level 6 you will be able to:	On achieving Level 5 you will be able to:	On achieving Level 4 you will be able to:
C1	**Work Independently** Exercise initiative, independence and personal responsibility to manage your own learning and time.	**Work Independently** Exercise independence and personal responsibility to manage your own learning and time.	**Work Independently** Manage your own learning and time.
C2	**Work with Others** Work collaboratively with others to achieve individual and common goals, solve problems creatively and build interpersonal relationships to flourish in a global workplace.	**Work with Others** Work collaboratively with others to achieve individual and common goals, solve problems creatively.	**Work with Others** Work collaboratively with others.
C3	**Communicate with Impact** Communicate clearly, effectively and impactfully with specialist and non-specialist audiences.	**Communicate with Impact** Communicate clearly and effectively with others.	**Communicate with Impact** Communicate accurately and reliably with others.
C4	**Demonstrate Digital Fluency** Use digital skills productively, critically and ethically to enhance creativity and communication.	**Demonstrate Digital Fluency** Use digital skills productively, critically and ethically.	**Demonstrate Digital Fluency** Use digital skills productively.

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.

Subject offered as single and/or combined award

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

BSc (Hons) Cyber Security				Status	
Level	Code	Title	Credits	Single	Joint
4	CYS4000-20	Fundamentals of Cyber Security	20	C	
4	CCO4000-20	CodeLab I	20	C	
4	CPU4002-20	Introduction to Computing	20	C	
4	CYS4001-20	Digital Forensics	20	C	
4	CPU4005-20	Databases	20	C	
4	CCO4007-20	Web Dev I	20	C	
5	CYS5000-20	Network Administration	20	C	
5	CPU5004-20	CodeLab II	20	C	
5	CYS5001-20	Intrusion Analysis and Response	20	C	
5	CYS5002-20	Cyber Resilience	20	C	
5	CCO5104-20	Web Dev II	20	O	
5	CPU5005-20	Software Engineering	20	O	
5	CPU5100-20	Data Visualisation	20	O	
5	CCO5105-20	Physical Computing	20	O	
5	CPU5006-20	Artificial Intelligence	20	O	
5	PPY5100-120	Professional Placement Year	120	O	
6	CYS6000-20	Cyber Crime, Law and Ethics	20	C	
6	CYS6001-20	Research Project	20	C	
6	CYS6002-20	Securing the Internet of Things	20	O	
6	CYS6003-20	Cyber Offence	20	C	
6	CYS6004-20	Cyber Defence	20	C	
6	CYS6005-20	Critical Infrastructure	20	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.

Please note: if you choose an optional module from outside this programme, you may be required to undertake a summative assessment task that does not appear in the assessment grid here in order to pass that module.

Work experience and placement opportunities

There are several opportunities to engage with industry across BSc (Hons) Cyber Security. We encourage you to take advantage of:

- Summer placement schemes
- Live briefs and industry pitching opportunities within modules
- Analytical and technical work as part of Cyber Security commissioned projects
- Roles within university-led external projects
- Invites to attend or participate in external networking opportunities, IT meetups and subject industry-insight events

BSc Cyber Security can also include a Professional Placement Year. The placement year is completed between years 2 and 3 of your degree and counts for 120 Level 5 credits. During this time you will be able to utilise knowledge gained as part of your studies in a real work environment to gain 'hands on' experience. The university has a dedicated Careers & Employability team to help you find and prepare for a placement. Following your placement year, you will return to University to complete your final year of study.

Opportunities to study abroad via International Exchange and Study Abroad programmes are also available.

Additional Costs Table

Module Code & Title	Type of Cost	Cost
CCO5105-20 Physical Computing	Students may wish to purchase additional physical computing components to develop their project ideas. The total additional costs will depend on the nature of the project.	£0-100

Graduate Attributes

Graduate Attribute	While at Bath Spa, I will develop my ability to:	This programme will help me to do this through:
Confidently Self-Aware	Reflect on and recognise my unique skills, strengths, and values and be able to apply and articulate them in a range of different contexts.	In Cyber Security we prepare students to meet the evolving challenges of protecting the digital systems and services through a blend of theory and practical work that cuts across knowledge in computing and cyber security, that engages tools and techniques employed in industry, and is supported by interaction with real-world business scenarios.
Emotionally Attuned	Be mindful of how my actions and emotions impact those around me so I can better navigate difficult situations and build effective interpersonal relationships.	During the course students engage in a variety of activities that support greater awareness of the context in which cyber security issues permeate businesses and society. These experiences help students to become emotionally attuned to the needs and drive of others in order to achieve successful outcomes.
Inclusive Collaborator	Contribute independently to collaborative projects while working effectively with others, valuing diversity and respecting individual differences.	The variety of assignment types and module tasks that require different perspectives to be considered in order to reach a consensus in a group. Through this process students learn to appreciate the beliefs of others and how they think, behave, and conduct themselves.
Adaptable Innovator	Embrace challenges, taking risks where needed and applying individual and collective problem solving.	The variety of assignment types and module tasks that require different perspectives to be considered in scenarios that have not been encountered previously. Students will be more confident in dealing with new situations and able to take the initiative.
Critical Thinker	Keep an open mind, ask curious questions and think creatively to gain a deeper and broader understanding of global perspectives and the world around me.	Students are encouraged to challenge conventional approaches and vendor solutions by assessing current threats and the technologies available to perpetrate attacks.
Forward Thinker	Set goals, plan ahead and utilise resources to support my personal ambitions and achieve my own version of success.	Students are constantly challenged to think about the changing nature of threats and approaches needed to combat them.
Ethical Leader	Act with empathy, making decisions grounded in ethical principles while advocating for sustainability and positive social change.	We ensure you consider the impact of actions you might take in prosecution of your duties so that the field of cyber security is respected and remains effective.

Responsible Self-Starter	Be accountable for my actions and decisions while demonstrating creativity, proactivity, and a focus on solutions.	Students are encouraged to make the use of the academic resources available to them, as well as external resources for the, to explore and experiment with. We provide networking with opportunities industry insights events hosting external speakers with their perspectives on success.
Compassionately Resilient	Respond to setbacks with a reflective and positive attitude, flexibility and a self-caring approach.	The majority of our time with students involve interactive, collaborative sessions, where we provide ongoing group and individual feedback on activities and assessments, in a safe and supportive environment.
Digitally Resourceful	Utilise and responsibly leverage existing and emerging technologies to solve problems and communicate.	The course aims to prepares you to meet the evolving challenges of protecting the digital systems and services we rely on in daily life. We use tools and techniques employed in the sector and cover the fundamental concepts and skills that underpin computing.

Modifications

Module-level modifications

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

Programme-level modifications

Nature of modification	Date(s) of approval and approving bodies	Date modification comes into effect
CCO4001-20 Web Development replaced with CCO4007-20 Web Dev I	Curriculum Committee December 2022	2023/24
CPU4001-20 The Computer Industry deleted	Curriculum Committee December 2022	2023/24
CPU4005-20 Databases added	Curriculum Committee December 2022	2023/24
CCO5000-20 CodeLab II replaced with CPU5004-20 CodeLab II	Curriculum Committee December 2022	2023/24
CCO5104-20 Web Dev II added	Curriculum Committee December 2022	2023/24
CPU5003-20 Software Project Management deleted	Curriculum Committee December 2022	2023/24
CCO5103-20 The Responsive Wed deleted	Curriculum Committee December 2022	2023/24
CPU5005-20 Software Engineering added as an Optional module	Curriculum Committee December 2022	2024/25
CYS5000-20 Network Administration changed to semester 2	Curriculum Committee December 2022	2024/25
CYS5002-20 Cyber Resilience changed to semester 1	Curriculum Committee December 2022	2024/25
Change of level 5 module Code Lab II to CPU5004-20 and change of course material alignment to Computing rather than creative computing	Curriculum Committee December 2022	2024/25
CPU5006-20 Artificial Intelligence added as an Optional module	Curriculum Committee December 2022	2024/25
CCO5105-20 Physical Computing added as an Optional module	Curriculum Committee December 2022	2024/25

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 – BSc (Hons) Cyber Security

Single Honours	
Level 4	
Semester 1	**Semester 2**

Single Honours	
Core Modules	
CCO4000-20 CodeLab I CPU4002-20 Introduction to Computing CYS4000-20 Fundamentals of Cyber Security	CCO4007-20 Web Dev I CPU4005-20 Databases CYS4001-20 Digital Forensics
Rule Notes: N/A	
Level 5	
Core Modules	
CPU5004-20 CodeLab II CYS5002-20 Cyber Resilience	CYS5000-20 Network Administration CYS5001-20 Intrusion Analysis and Response
Optional Modules	
CCO5104-20 Web Dev II CPU5006-20 Artificial Intelligence	CPU5100-20 Data Visualisation CCO5105-20 Physical Computing CPU5005-20 Software Engineering
Rule Notes: N/A	
Optional Professional Placement Year 120 credits	
Level 6	
Core Modules	
CYS6000-20 Cyber Crime, Law and Ethics CYS6001-20 Research Project	CYS6003-20 Cyber Offence CYS6004-20 Cyber Defence CYS6005-20 Critical Infrastructure
Optional Modules	
CYS6002-20 Securing the Internet of Things	
Rule Notes: N/A	

Appendix 2: Map of Intended Learning Outcomes

Level	Module Code	Module Title	Status	Intended Learning Outcomes														
			(C,R,R*,O) [4]	Subject-specific Skills and Knowledge							Cognitive and Intellectual Skills				Skills for Life and Work			
				A1	A2	A3	A4	A5	A6	A7	B1	B2	B3	B4	C1	C2	C3	C4
4	CYS4000-20	Fundamentals of Cyber Security	C	x	x			x	x		x		x	x	x		x	
4	CCO4000-20	CodeLab I	C			x	x			x		x			x	x	x	x
4	CPU4002-20	Introduction to Computing	C			x		x	x	x	x	x		x	x	x	x	x
4	CYS4001-20	Digital Forensics	C		x		x	x	x	x	x	x		x	x	x	x	x
4	CCO4007-20	Web Dev I	C			x	x			x		x			x	x	x	x
4	CPU4005-20	Databases	C			x	x				x				x		x	x
5	CYS5000-20	Network Administration	C	x		x	x			x	x	x			x	x		x
5	CPU5004-20	CodeLab II	C			x	x					x			x		x	x
5	CYS5001-20	Intrusion Analysis and Response	C	x	x	x	x	x	x	x	x	x		x	x		x	x
5	CYS5002-20	Cyber Resilience	C		x	x		x	x	x	x		x	x	x	x	x	x
5	CCO5104-20	Web Dev II	O	x			x					x	x		x		x	x
5	CPU5005-20	Software Engineering	O	x			x					x	x	x	x	x	x	x
5	CPU5100-20	Data Visualisation	O	x			x			x		x	x		x		x	x
5	CCO5105-20	Physical Computing	O				x			x		x	x		x		x	x
5	CPU5006-20	Artificial Intelligence	O			x	x			x	x	x	x		x		x	x
5	PPY5100-120	Professional Placement Year	O												x	x	x	x
6	CYS6000-20	Cyber Crime, Law and Ethics	C	x	x						x		x		x		x	
6	CYS6001-20	Research Project	C	x				x			x		x		x		x	
6	CYS6002-20	Securing the Internet of Things	O	x		x	x	x		x	x	x		x	x			x
6	CYS6003-20	Cyber Offence	C	x	x	x	x	x		x	x	x			x	x		x
6	CYS6004-20	Cyber Defence	C	x	x	x	x	x	x	x	x	x		x	x	x	x	x
6	CYS6005-20	Critical Infrastructure	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) [5]	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)
4	CYS4000-20	Fundamentals of Cyber Security	C			1x							1x				
4	CCO4000-20	CodeLab I	C						1x		1x			1x			
4	CPU4002-20	Introduction to Computing	C			1x					1x				1x		
4	CYS4001-20	Digital Forensics	C						1x					1x			
4	CCO4007-20	Web Dev I	C						1x					1x			
4	CPU4005-20	Databases	C								2x						
5	CYS5000-20	Network Administration	C						1x					1x			
5	CPU5004-20	CodeLab II	C						1x		1x	1x					
5	CYS5001-20	Intrusion Analysis and Response	C						2x								
5	CYS5002-20	Cyber Resilience	C					1x									
5	CCO5104-20	Web Dev II	O								2x						
5	CPU5005-20	Software Engineering	O						1x		1x		1x				
5	CPU5100-20	Data Visualisation	O					1x					1x				
5	CCO5105-20	Physical Computing	O					1x									
5	CPU5006-20	Artificial Intelligence	O								2x						
5	PPY5100-120	Professional Placement Year	O					1x	1x								
6	CYS6000-20	Cyber Crime, Law and Ethics	C					1x			1x						
6	CYS6001-20	Research Project	C			1x							1x				
6	CYS6002-20	Securing the Internet of Things	O					1x	1x								
6	CYS6003-20	Cyber Offence	C					1x									
6	CYS6004-20	Cyber Defence	C					1x									
6	CYS6005-20	Critical Infrastructure	C						1x				1x				

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