BATH SPA UNIVERSITY

Definitive Programme Document: Cyber Security

(Bachelor’s of Science with Honours)

Awarding institution	Bath Spa University
Teaching institution	Bath Spa University
School	School of Design
Main campus	Newton Park
Other sites of delivery	N/A
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
Professional Placement Year	Yes
Duration of award	3 years full-time (4 years with Professional Placement Year)
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)	
Relevant QAA Subject Benchmark Statements (including date of publication)	Computing (October 2019)
Date of most recent approval	31 March 2021
Date specification last updated	October 2021

Exemptions

There are no exemptions.

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

[2] See section on '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	Law, Regulation and Ethics - the ability to critically evaluate the legal	Law, Regulation and Ethics - Knowledge of key laws, regulation and

	regulation, and the ability to critically examine the legal and ethical implications of decisions in cyber security, including instances that present moral conflict.	and regulatory underpinnings and ethical dimension of key professional roles in the field of cyber security.	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

	Programme Intended Learning Outcomes (ILOs) On Achieving Level 6	**On Achieving Level 5**	**On Achieving Level 4**
C1	Autonomous learning[3] (including time management) that shows the exercise of initiative and personal responsibility and enables decision-making in complex and unpredictable contexts.	Autonomous learning (including time management) as would be necessary for employment requiring the exercise of personal responsibility and decision-making such that significant responsibility within organisations could be assumed.	Autonomous learning (including time management) as would be necessary for employment requiring the exercise of personal responsibility.
C2	Team working skills necessary to flourish in the global workplace with the ability both to work in and lead teams effectively.	Team work as would be necessary for employment requiring the exercise of personal responsibility and decision-making for effective work with others such that significant responsibility within organisations could be assumed.	Team work as would be necessary for employment requiring the exercise of personal responsibility for effective work with others.
C3	Communication skills that ensure information, ideas, problems and solutions are communicated effectively and clearly to both specialist and non-specialist audiences.	Communication skills commensurate with the effective communication of information, arguments and analysis in a variety of forms to specialist and non-specialist audiences in which key techniques of the discipline are deployed effectively.	Communication skills that demonstrate the ability to communicate outcomes accurately and reliably and with structured and coherent arguments.
C4	IT skills and digital literacy that demonstrate core competencies and are commensurate with the ability to work at the interface of creativity and new technologies.	IT skills and digital literacy that demonstrate the development of existing skills and the acquisition of new competences.	IT skills and digital literacy that provide a platform from which further training can be undertaken to enable development of new skills within a structured and managed environment.

[3] i.e. the ability to review, direct and manage one’s own workload

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.

BSc (Hons) Computing				Status			
Level	Code	Title	Credits	Single	Major	Joint	Minor
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	CPU4001-20	The Computer Industry	20	C			
4	CCO4001-20	Web Development	20	C			
5	CYS5000-20	Network Administration	20	C			
5	CCO5000-20	CodeLab II	20	C			
5	CPU5002-20	Databases	20	C			
5	CYS5001-20	Intrusion Analysis and Response	20	C			
5	CYS5002-20	Cyber Resilience	20	C			
5	CPU5003-20	Software Project Management	20	O			
5	CCO5103-20	The Responsive Web	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	20	O			

		Internet of Things					
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.

Graduate Attributes

	Bath Spa Graduates…	In BSc (Hons) Cyber Security, we enable this by…
1	Will be employable: equipped with the skills necessary to flourish in the global workplace, able to work in and lead teams	Approaching cyber security from a holistic perspective to encourage interaction with multiple aspects of the field, and their respective professional roles.
2	Will be able to understand and manage complexity, diversity and change	Exposing the rate at which computing and cyber security move as applied subjects, and assisting students to establish strategies for maintaining pace.
3	Will be creative: able to innovate and to solve problems by working across disciplines as professional or artistic practitioners	Helping students establish computational thinking and analytical thinking skills to support the application of their technical skills.
4	Will be digitally literate: able to work at the interface of creativity and technology	Recognising the inseparable connection between computing and cyber security, and teaching not only specific applied skills required by employers but also the technical foundations of these subjects.
5	Will be internationally networked: either by studying abroad for part of their programme, or studying alongside students from overseas	Engaging cyber security as an international concern, and by seeking and facilitating opportunities for knowledge exchange with specialist speakers and learners located outside of the UK.
6	Will be creative problem solvers, doers and makers	Assisting students in developing the innovative mindset needed to contribute to efforts that will drive the cyber sector forward.
7	Will be critical thinkers: able to express their ideas in written and oral form, and possessing information literacy	Facilitating critical engagement with a range of credible sources and perspectives in the cyber security sector, and ensuring methods of assessment cover multiple forms of communication, with each having a specific function in the field.
8	Will be ethically aware: prepared for citizenship in a local, national and global context	Embedding in the course multiple points of interaction with the ethical dimension of cyber security, including instances of tension between the values of society and the operational needs of organisations.

Modifications

Module-level modifications

Code	Title	Nature of modification	Date(s) of approval and approving bodies	Date modification comes into effect
CCO5103-20	The Responsive Web	ILO updates	TBC	2022/23

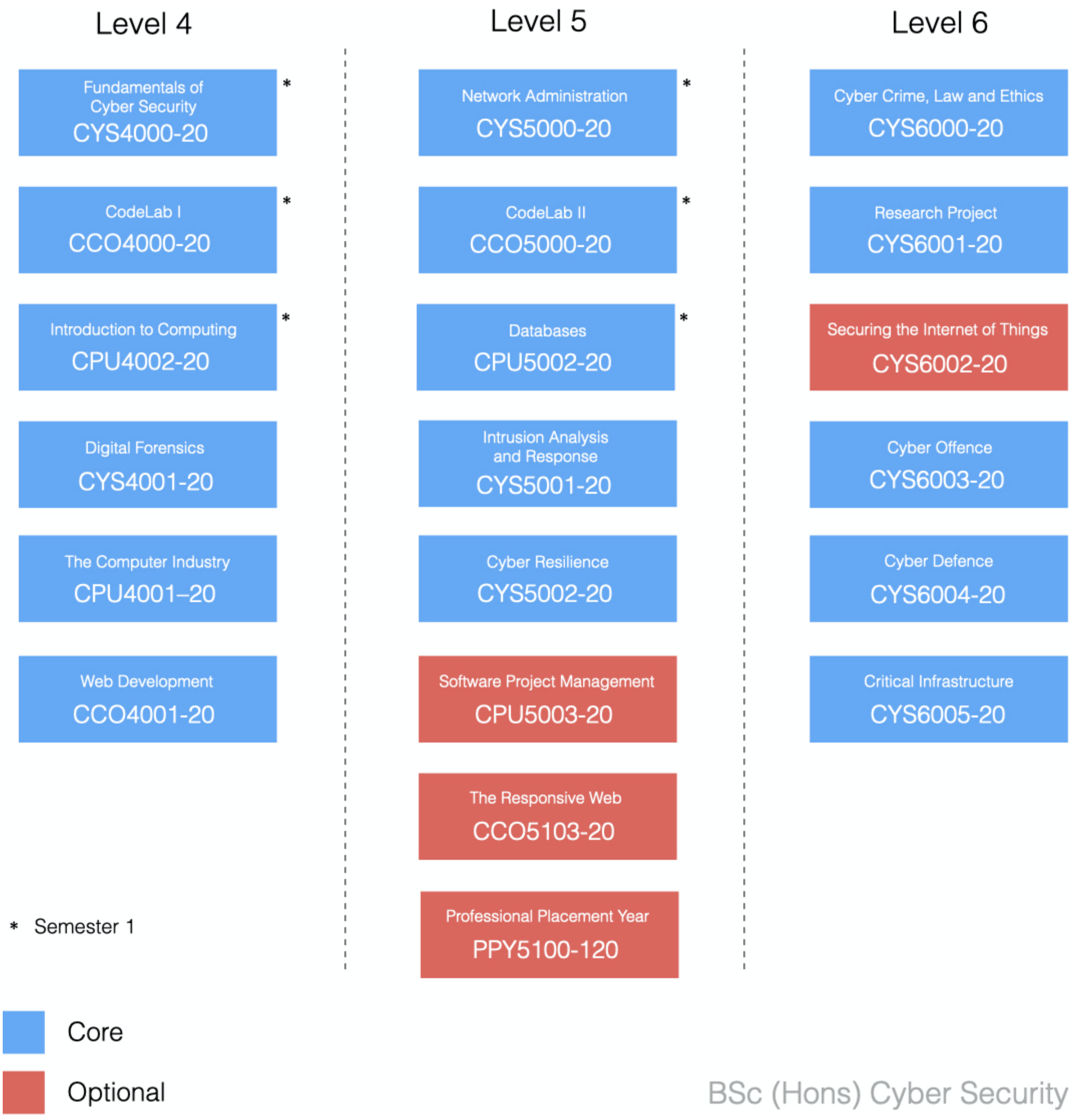
Programme-level modifications

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



Level 4

Fundamentals of Cyber Security CYS4000-20 *

CodeLab I CCO4000-20 *

Introduction to Computing CPU4002-20 *

Digital Forensics CYS4001-20

The Computer Industry CPU4001–20

Web Development CCO4001-20

Level 5

Network Administration CYS5000-20 *

CodeLab II CCO5000-20 *

Databases CPU5002-20 *

Intrusion Analysis and Response CYS5001-20

Cyber Resilience CYS5002-20

Software Project Management CPU5003-20

The Responsive Web CCO5103-20

Professional Placement Year PPY5100-120

Level 6

Cyber Crime, Law and Ethics CYS6000-20 *

Research Project CYS6001-20 *

Securing the Internet of Things CYS6002-20 *

Cyber Offence CYS6003-20

Cyber Defence CYS6004-20

Critical Infrastructure CYS6005-20

* Semester 1

🟦 Core

🟥 Optional

BSc (Hons) Cyber Security

Appendix 2: Map of Intended Learning Outcomes (ILOs) against modules

BSc (Hons) Cyber Security

Level	Module Code	Module Title	Status (C,R,R*,O)[4]	Intended Learning Outcomes														
				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	✓	✓			✓	✓		✓		✓	✓	✓		✓	
4	CCO4000-20	CodeLab I	C			✓	✓			✓		✓			✓	✓	✓	✓
4	CPU4002-20	Introduction to Computing	C			✓						✓	✓		✓		✓	
4	CYS4001-20	Digital Forensics	C		✓		✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
4	CPU4001-20	The Computer Industry	C	✓	✓						✓		✓		✓		✓	
4	CCO4001-20	Web Development	C			✓	✓			✓		✓			✓	✓	✓	✓
5	CYS5000-20	Network Administration	C	✓		✓	✓			✓	✓	✓			✓	✓		✓
5	CCO5000-20	CodeLab II	C			✓	✓					✓			✓		✓	✓

5	CYS5001-20	Intrusion Analysis and Response	C	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓		✓	✓
5	CYS5002-20	Cyber Resilience	C		✓	✓		✓	✓	✓	✓		✓	✓	✓	✓	✓	✓
5	CPU5003-20	Software Project Management	O	✓		✓	✓					✓	✓	✓	✓	✓	✓	✓
5	CCO5103-20	The Responsive Web	O			✓	✓					✓			✓			✓
5	PPY5100-120	Professional Placement Year	O												✓	✓	✓	✓
6	CYS6000-20	Cyber Crime, Law and Ethics	C	✓	✓						✓		✓		✓		✓	
6	CYS6001-20	Research Project	C	✓				✓			✓		✓		✓		✓	
6	CYS6002-20	Securing the Internet of Things	O	✓		✓	✓	✓		✓	✓	✓		✓	✓			✓
6	CYS6003-20	Cyber Offence	C	✓	✓	✓	✓	✓		✓	✓	✓			✓	✓		✓
6	CYS6004-20	Cyber Defence	C	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
6	CYS6005-20	Critical Infrastructure	C	✓		✓		✓	✓	✓	✓			✓	✓	✓	✓	

Appendix 3: Map of summative assessment tasks by module

BSc (Hons) Cyber Security

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	CPU4001-20	The Computer Industry	C						1x		1x		1x				
4	CCO4001-20	Web Development	C						1x		1x			1x			
5	CYS5000-20	Network Administration	C						1x					1x			

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

5	CCO5000-20	CodeLab II	C						1x		1x	1x					
5	CPU5002-20	Databases	C								2x						
5	CYS5001-20	Intrusion Analysis and Response	C						2x								
5	CYS5002-20	Cyber Resilience	C					1x									
5	CPU5003-20	Software Project Management	O						1x				1x				
5	CCO5103-20	The Responsive Web	O						1x		1x			1x			
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				

Appendix 4: Module Descriptors

1	Module code	CYS4000-20			
2	Module title	Fundamentals of Cyber Security			
3	Subject	Cyber Security			
4	Core, Required or Required* for	BSc (Hons) Cyber Security			
5	Level	**4**	5	6	7
6	UK credits	20			
7	ECTS credits	10			
8	Optional for	N/A			
9	Excluded combinations	N/A			
10	Pre-requisite or co-requisite	N/A			
11	Class contact time: total hours	Total Hours: 52			
12	Independent study time: total hours	Total Hours: 148			
13	Semester(s) of delivery	Semester 1			
14	Main campus location	Newton Park			
15	Module co-ordinator	John Curry			
16	Additional costs involved	N/A			

17 **Brief description and aims of module**

Cyber security has been defined as one of the key threats to the prosperity of the United Kingdom by the government, while similar conclusions have been drawn across the globe. The threat to individuals, businesses and the public sector has never been greater.

The module is to place your studies in context by giving you a holistic understanding of the scope and depth of the cyber security sector. You are introduced to all key concerns of the subject - from identification and detection of threats through to response and recovery - using case studies to underpin relevance and significance. We examine how the field has emerged, how it has evolved, and what paths it may take in the future. With a focus on potential roles within the sector, you build critical knowledge of how cyber security principles are embedded into enterprise systems.

18 **Outline syllabus**

- The origins and evolution of cyber security
- Disciplines within cyber security and key roles
- The five functions - identify, protect, detect, respond, recover
- Defence in depth
- Understanding human factors
- Routine attack and defence methods
- Case study analysis
- The future of cyber security

19 **Teaching and learning activities**

Class Hours

Lectures introduce key theories and principles in cyber security. Seminars offer an opportunity to gather and discuss perspectives on essential topics with support from

	case study analysis. *Independent Learning* Gaining critical insight into cyber security requires not only an examination of core material but also up-to-date knowledge of current affairs. You are asked to keep track of developments in cyber security via online sources as well as fortify and extend your understanding of topics covered in class.	
20	**Intended learning outcomes** *By successful completion of the module, you will be able to demonstrate*	*How assessed*
	1. Knowledge of the core concepts and principles that underpin the field of cyber security.	F2, S1, S2
	2. An understanding of widely recognised roles in the cyber security sector and the objectives of such roles.	F1, S1
	3. Knowledge of routine cyber threats to businesses and the public sector.	F2, S2
	4. The ability to extract insights on the key concerns of the cyber security sector from case study analysis.	F2, S2
21	**Assessment and feedback** *Formative exercises and tasks:* F1. Role analysis exercise. F2. Five minute essays.	
	Summative assessments:	Weighting
	S1. Presentation. On a role in the cyber security sector (15 minutes, group).	30%
	S2. Cyber fundamentals essay (2,800 words).	70%
22	**Learning resources** *University Library print, electronic resources and Minerva:* *Key texts:* ● Augenbaum, S. (2019) *The secret to cybersecurity: a simple plan to protect your family and business from cybercrime*. Forefront Books. ● Caravelli, J and Jones, N. (2019) *Cyber security: threats and responses for government and business*. Praeger. ● Meeuwisse, R. (2017) *Cyber security for beginners*. Cyber Simplicity Ltd ● Ozkaya, E. (2019) *Cybersecurity: the beginner's guide: a comprehensive guide to getting started in cybersecurity*. Packt Publishing. *Key web-based and electronic resources:*	

	● The Register (cyber security news) - www.theregister.co.uk/security ● Get Safe Online, (government advice site) - www.getsafeonline.org ● Future Learn course, Introduction to Cyber Security - https://www.futurelearn.com/courses/introduction-to-cyber-security ● National Cyber Security Centre (NCSC) - www.ncsc.gov.uk ● NCSC weekly threat reports - https://www.ncsc.gov.uk/section/keep-up-to-date/threat-reports ● NIST Cyber Security Framework - https://www.nist.gov/cyberframework ● The Hacker News - https://thehackernews.com ● IT Security Guru (IT security news stories) - https://www.itsecurityguru.org ● Linkedin Learning courses and videos related to cyber security fundamentals. Accessible via the Bath Spa Library website - https://www.bathspa.ac.uk/library/library-databases ● Immersive Labs. Access provided for free if signing up using BSU email address - http://immersivelabs.online/
23	**Preparatory work** Take some time to consider how cyber security has an effect on your life. Make a list of where you encounter cyber security measures, and think about the trade-off between level of protection and convenience. It would be useful for you to read BBC news stories on the topic of cyber security for a flavour of current concerns in the UK. The US publication Politico is worth visiting online.

1	Module code	CCO4000-20			
2	Module title	CodeLab I			
3	Subject	Creative Computing			
4	Core, Required or Required* for	BSc (Hons) Creative Computing (Animation) BSc (Hons) Creative Computing (Gaming) BSc (Hons) Creative Computing (Web Technologies) BSc (Hons) Creative Computing Joint BSc (Hons) Computing BA (Hons) Games Development BSc (Hons) Cyber Security			
5	Level	**4**	5	6	7
6	UK credits	20			
7	ECTS credits	10			
8	Optional for	N/A			
9	Excluded combinations	N/A			
10	Pre-requisite or co-requisite	N/A			
11	Class contact time: total hours	Total Hours: 52			
12	Independent study time: total hours	Total Hours: 148			
13	Semester(s) of delivery	Semester 1			
14	Main campus location	Newton Park			
15	Module co-ordinator	Jake Hobbs			
16	Additional costs involved	N/A			

17 **Brief description and aims of module**

CodeLab I is a rapid prototyping workshop series that introduces the fundamentals of procedural programming. You encounter the first principles of coding from computational thinking and maths for programmers to key elements such as variables, conditionals, loops, arrays and functions.

We assume little to no prior experience of coding on entry. You learn procedural programming from the ground up, working through coding challenges and creative briefs that help embed new techniques and best practice into your programming ‘toolkit’.

18 **Outline syllabus**

- Computational thinking
- Version Control Basics
- Data types and operators
- Conditionals
- Loops
- Arrays
- Functions
- Control flow
- Project planning
- Coding convention and troubleshooting

19 **Teaching and learning activities**

Class Hours

Codelab I adopts the principle of 'learning by making'. Teaching time includes bite size code demonstrations (to present new techniques), logic challenges, prototyping workshops (to test ideas) and code review sessions. Logic challenges and longer-running projects are undertaken both individually and in small groups. Learning takes place initially via manual games and puzzles before migrating to industry-standard code editors. Through the module you are required to compile a 'code repository' using the web-based service GitHub. The repository is a useful tool for keeping track of specific coding techniques and managing your projects.

Independent Learning

Learning to program is comparable to learning to communicate in a second language. It requires practice, persistence and time to become proficient. It is therefore important that you make the most of your independent study time to revisit techniques and search out new ones. Be inquisitive, creative and have fun - this is the easiest way to get to grips with code. Anyone can learn how to program.

20	**Intended learning outcomes** *By successful completion of the module, you will be able to demonstrate*	*How assessed*
	1. An understanding of the key features of programming including input, output, maths, sequence, iteration and repetition.	F1, S1
	2. The application of coding conventions to ease the review, maintenance, troubleshooting and debugging of developed software.	F1, S1, S2
	3. The successful implementation of a prototype system that is driven by procedural programming techniques.	F1, S2
	4. The ability to specify applications, discuss their technical implementation and reflect critically on the results.	F1, S2

21	**Assessment and feedback** *Formative exercises and tasks:*	
	F1. In-class quizzes and logic challenges.	
	Summative assessments:	Weighting
	S1. Programming skills portfolio.	40%
	S2. Utility app. With supporting documentation.	60%

22 **Learning resources**

University Library print, electronic resources and Minerva:

Key texts:

- Beecher, K. (2018). *Bad programming practices 101: become a better coder by learning how (not) to program* (e-book). Apress
- Beecher, K. (2017). *Computational thinking: a beginner’s guide to problem-solving and programming*. BCS.
- Kowalski, R. (2011). *Computational logic human thinking* (e-book). Cambridge University Press.
- Savitch, W & Mock, K. (2015). *Problem solving with C++, global edition* (e-book). Pearson Education.
- Stroustrup, B. (2014). *Programming: principles and practice using C++.* Addison-Wesley

Key web-based and electronic resources:

- LinkedIn Learning resources related to procedural programming. Accessible via the Bath Spa Library website - https://www.bathspa.ac.uk/library/library-databases

Specialist resources:

- GitHub Desktop (cross-platform, free) - https://desktop.github.com
- Visual Studio (cross-platform, free) - https://www.visualstudio.com
- XCode (Mac, free) - https://developer.apple.com/xcode

23 **Preparatory work**

This module requires no previous experience of programming. You may however wish to browse LinkedIn Learning tutorials on C++ for a flavour of what the module covers.

1	Module code	CPU4002-20			
2	Module title	Introduction to Computing			
3	Subject	Computing			
4	Core, Required or Required* for	BSc (Hons) Computing BSc (Hons) Cyber Security			
5	Level	**4**	5	6	7
6	UK credits	20			
7	ECTS credits	10			
8	Optional for	N/A			
9	Excluded combinations	N/A			
10	Pre-requisite or co-requisite	N/A			
11	Class contact time: total hours	Total Hours: 52			
12	Independent study time: total hours	Total Hours: 148			
13	Semester(s) of delivery	Semester 1			
14	Main campus location	Newton Park			
15	Module co-ordinator	Dave Cobb			
16	Additional costs involved	N/A			

17 **Brief description and aims of module**

Computer Science is all about effective problem solving using data. But what, exactly, is data, and what do we need to know about it? How can we use it? What problems can there be in its use and storage? In this module you will learn what data is, how it is represented, manipulated, processed, stored, transferred, error-checked and compressed. You will learn how to elicit, represent and analyse the flow of data through systems, and how systems are effectively developed. You will gain an understanding of the devices, software and protocols that are used to do this, as well as the associated social and legal implications.

18 **Outline syllabus**

- A brief history of computing
- Raw data (binary, hex, bits, bytes)
- Computer components and what they do (CPU, RAM, ROM, drivers)
- Memory
- Operating systems
- Networks (technologies, topologies, the OSI Model)
- The Internet
- The fetch-execute cycle
- Modelling specifications
- Human computer interaction (respecting the user)
- The safe, secure and ethical use of computing
- The future of computing and data

19 **Teaching and learning activities**

Class Hours

Learning is seminar based with individual and group activities where appropriate. The computer science aspects of the module adopt a lecture format, complemented by flipped classroom research exercises and in-class quizzes. The sessions that place computing in a wider context are less didactic, and promote free and open discussion

	on the topics covered. The aim is to debate the pros and cons of contemporary computing, rather than to advocate a particular perspective. *Independent Learning* Each week we provide you with seminar presentations (with notes) and links to further reading. It is good practice to get into a routine of exploring these materials, and giving yourself enough time to follow up on topics that particularly interest you or require further clarification. You are advised also to seek an overview of each lecture topic before you attend class (see resources or conduct a web search) to help add context to the session.	
20	**Intended learning outcomes** *By successful completion of the module, you will be able to demonstrate:*	*How assessed*
	1. Knowledge of the core features of contemporary computing systems.	F1, S1
	2. Skills in interpreting, manipulating and representing data.	F1, S1
	3. Engagement with the key social, ethical, cultural and legal consequences of computing.	F1, S2
	4. The ability to locate, assess and consolidate information in the field of computer science from print and online resources.	F1, S2
21	**Assessment and feedback** *Formative exercises and tasks:*	
	F1. In-class quizzes and logic challenges.	
	Summative assessments:	Weighting
	S1. Exam. On computer science topics (2 hours).	50%
	S2. Research project (2,000 words).	50%
22	**Learning resources** *University Library print, electronic resources and Minerva:* *Key texts:* ● Ceruzzi, P. (2012) *Computing: a concise history* (e-book). MIT Press. ● McCosker, A., Vivienne, S. & Johns, A. (2016). *Negotiating digital citizenship* (e-book). Rowman & Littlefield International. ● Mossberger, K. (2008) *Digital citizenship: the Internet, society, and participation* (e-book). MIT Press. ● Quinn, M. (2015) *Ethics for the information age* (e-book). Addison Wesley. ● Ribble, M. (2015) *Digital citizenship in schools: nine elements all students should know* (e-book). International Society for technology in Education. ● Ryan, J. (2010) *A History of the Internet and the digital future* (e-book).	

	Reaktion Books. ● Stallings, W. (2015) *Operating systems: internals and design principles* (e-book). Pearson. ● Wempen, F. et al. (2014) *Computing fundamentals* (e-book). John Wiley & Sons. *Web-based and electronic resources:* ● TutorialsPoint, overview of Hardware, Operating Systems and Networking – http://www.tutorialspoint.com/computer_fundamentals/index.htm ● Harvard Video Series, understanding computers and the Internet video series – http://computerscience1.tv/2011/spring ● A brief history of computer ethics – http://stanford.library.usyd.edu.au/archives/spr2006/entries/ethics-computer ● Long live the web: a call for continued open standards and neutrality by Tim Berner's Lee – https://www.scientificamerican.com/article/long-live-the-web
23	**Preparatory work** You should browse the TutorialsPoint and Harvard Video Series resources listed above. Both offer an excellent overview of many of the topics covered in *Introduction to Computing*.

1	Module code	CYS4001-20			
2	Module title	Digital Forensics			
3	Subject	Cyber Security			
4	Core, Required or Required* for	BSc (Hons) Cyber Security			
5	Level	**4**	5	6	7
6	UK credits	20			
7	ECTS credits	10			
8	Optional for	N/A			
9	Excluded combinations	N/A			
10	Pre-requisite or co-requisite	N/A			
11	Class contact time: total hours	Total Hours: 52			
12	Independent study time: total hours	Total Hours: 148			
13	Semester(s) of delivery	Semester 2			
14	Main campus location	Newton Park			
15	Module co-ordinator	Ian Wills			
16	Additional costs involved	N/A			

17 **Brief description and aims of module**

Digital forensics concerns techniques for recovering and analysing material found on computing devices. Often leveraged to investigate instances of cyber crime but also network intrusion and other forms of legal dispute, the field has in recent years gained significant relevance for both the private and public sector. Having a good understanding of the methods, objectives and limitations of digital forensics is essential for cyber security practitioners. As well as helping to identify malicious activity, forensic work supports fortification of business IT policies, and with it, mitigation of future cyber attacks.

This module covers the fundamentals of digital forensics, beginning with what it is and what it's used for. We go on to examine a number of investigative tools and key techniques for collecting and analysing data from digital devices, as well as the human intuition that must be employed to identify evidence and draw conclusions from it. During this, you may be surprised by the type of scope of information that may be retrieved about a user's specific activity, and more generally, their digital footprint. The module is structured to engage the five stages of digital forensics - identification, preservation, collection, analysis and reporting. These steps are engaged as necessary with reference to the laws and regulations that govern the field.

18 **Outline syllabus**

- The origins of digital forensics
- The utility of digital forensics and role of investigators
- The digital forensics process: identification, preservation, collection, analysis and reporting
- Key tools for digital forensics (open source and commercial)
- Evidence handling
- Laws, regulation and rules of evidence

19 **Teaching and learning activities**

Class Hours

Lectures and seminars discuss key concepts in digital forensics, supported by relevant case study materials. Workshops introduce key tools for digital forensics and examine their application in varying investigative scenarios.

Independent Learning

You are expected to conduct readings and digital forensics tasks set by tutors outside of class hours. As digital forensics is a scientific process, albeit one that is backed up by human intuition, it is important to engage set exercises to become familiar with methods of ensuring integrity of evidence.

20 **Intended learning outcomes**
By successful completion of the module, you will be able to demonstrate

	How assessed
1. Knowledge of the objectives of digital forensics and the stages of the digital forensics process.	F1, S1, S2
2. The ability to collect and analyse data from digital devices using key tools for forensic investigation.	F1, S1, S2
3. Awareness of the laws and regulations that govern the field of digital forensics, and their effects on investigative procedure.	F2, S1, S2
4. The ability to draw on established methods in the field of digital forensics to establish and report evidence.	F2, S2

Assessment and feedback
Formative exercises and tasks:

F1. Investigative challenges.

F2. Evidence handling exercise.

Summative assessments:	Weighting
S1. Digital forensics set exercises.	40%
S2. Forensic investigation (2,400 words).	60%

21 **Learning resources**
University Library print, electronic resources and Minerva:

Key texts:

- Hassan, N. A. (2019) *Digital forensics basics: a practical guide using Windows OS*. Apress.
- Hayes, D. (2020) *A practical guide to digital forensics investigations*. Pearson.
- Oettinger, W. (2020) *Learn computer forensics: A beginner's guide to searching, analyzing, and securing digital evidence*. Packt Publishing.

	Key web-based and electronic resources: ● DFRWS (Digital Forensics Research Workshop) - https://dfrws.org ● Cyber Forensicator - http://cyberforensicator.com/ ● SANS Blog: digital forensics and incident response - https://www.sans.org/blog/?focus-area=digital-forensics ● LinkedIn Learning videos and courses related to digital forensics. Accessible via the Bath Spa Library website - https://www.bathspa.ac.uk/library/library-databases *Specialist resources:* ● The Sleuth Kit/Autopsy (open source digital forensics tools) - http://www.sleuthkit.org/autopsy ● Tools to examine browser history ● Various password cracking tools
22	**Preparatory work** Read and make notes on chapter 1 of Darren Hayes' *A practical guide to digital forensics investigations* for an understanding to the scope of the topic. The text is available as an e-resource in the Bath Spa library catalogue - https://www.bathspa.ac.uk/library

1	Module code	CPU4001-20			
2	Module title	The Computer Industry			
3	Subject	Computing			
4	Core, Required or Required* for	BSc (Hons) Computing BSc (Hons) Cyber Security			
5	Level	**4**	5	6	7
6	UK credits	20			
7	ECTS credits	10			
8	Optional for	N/A			
9	Excluded combinations	N/A			
10	Pre-requisite or co-requisite	N/A			
11	Class contact time: total hours	Total Hours: 52			
12	Independent study time: total hours	Total Hours: 148			
13	Semester(s) of delivery	Semester 2			
14	Main campus location	Newton Park			
15	Module co-ordinator	Dave Cobb			
16	Additional costs involved	N/A			
17	**Brief description and aims of module** The computer industry comprises a wide range of professional activities that include (but are not limited to) system and application development, problem solving using technology, and related support services. Employers range greatly in scale and breadth, cutting across financial, retail, entertainment, telecommunications and public sectors, to name just a few. The computer industry grows and evolves at a rapid pace, which poses a number of significant local and national challenges for business leaders and policy makers. Such challenges range from addressing the perceived ‘skills gap’ - both within companies and at large - to responding to wider shifts in politics and the economy or to emerging data protection and security concerns. This module acts as a forum for discussion and evaluation on the *state of play* of the IT industry (roles, goals and challenges), therefore providing valuable insight for individuals looking to enter the computer sector. The UK industry is outward looking and international, therefore it is also important to investigate the rapidly expanding overseas marketplaces such as those in China, India, South Korea, the US and Japan. Local context is also reviewed, leading to a scoping of the variety and focus of IT businesses within the South West. The objective of this aspect is to help you develop an understanding of potential routes to employment regionally, while identifying the skills and qualities that you need to succeed in the computer sector.					
18	**Outline syllabus** ● The scale and scope of the computer industry ● Job roles and responsibilities ● Historical ‘game changers’ ● Current commercial trends ● Emerging challenges, concerns and threats (UK) ● An overview of the international IT marketplace ● External influences and their consequences ● Unpacking the computer industry - regionally, nationally and internationally ● Sustainable computing					

19	**Teaching and learning activities** *Class Hours* Seminar sessions are discursive, with a strong emphasis on individual and group research. You are asked to evaluate aspects of the computer industry regularly, and to present your findings in a number of forms (formal presentation, roundtables and debates). *Independent Learning* You are expected to conduct data gathering exercises outside of class hours, as well as engage the reading materials set by tutors.	
20	**Intended learning outcomes** *By successful completion of the module, you will be able to demonstrate:*	*How assessed*
	1. Knowledge of the types of business within the computer industry and their respective job roles and responsibilities.	F1, S1, S2
	2. The ability to discuss critically, factors that shape the trajectory of the computer industry.	F1, S2
	3. An understanding of the scale and scope of the South West computer industry.	F1, S1
	4. Awareness of the importance of sustainability in respect to the computer industry.	F1, S2
21	**Assessment and feedback** *Formative exercises and tasks:* F1. Group presentation on a specific computing business type.	
	Summative assessments:	Weighting
	S1. Visualisation of the South West computer industry (with presentation).	40%
	S2. Strategy statement (2,400 words).	60%
22	**Learning resources** *University Library print, electronic resources and Minerva:* *Key texts:* ● Yost, J., Aspray, W. & Misa, T. (2017) *Making IT work: a history of the computer services industry* (e-book). MIT Press. ● Cortada, J., Aspray, W. & Misa, T. (2019) *IBM: the rise and fall and reinvention of a global icon.* MIT Press.	

	Key web-based and electronic resources: ● The Economist. Accessible through Bath Spa Library - https://www.bathspa.ac.uk/library/ ● The Register, IT news and analysis – https://www.theregister.co.uk ● The Verge, tech section – https://www.theverge.com/tech ● We encourage students to become members of the British Computer Society (BCS) to gain access to a wealth of resources around the computer industry. Information on a annual subscription for student can be found at https://www.bcs.org/membership/become-a-member/students-and-apprentices/ (£20 per year at the time of writing) ● ITNOW – the magazine for the IT professional (offered as part of a BCS subscription)
23	**Preparatory work** Select one type of business within the computer industry (e.g. component manufacture, IT security, consultancy) and create a short overview of two companies in the UK or abroad that specialise in this area.

1	Module code	CCO4001-20
2	Module title	Web Development
3	Subject	Creative Computing
4	Core, Required or Required* for	BSc (Hons) Creative Computing (Animation) BSc (Hons) Creative Computing (Gaming) BSc (Hons) Creative Computing (Web Technologies) BSc (Hons) Creative Computing Joint BSc (Hons) Computing BSc (Hons) Cyber Security
5	Level	**4** 5 6 7
6	UK credits	20
7	ECTS credits	10
8	Optional for	Core
9	Excluded combinations	N/A
10	Pre-requisite or co-requisite	N/A
11	Class contact time: total hours	Total Hours: 52
12	Independent study time: total hours	Total Hours: 148
13	Semester(s) of delivery	Semester 2
14	Main campus location	Newton Park
15	Module co-ordinator	Jake Hobbs
16	Additional costs involved	None
17	**Brief description and aims of module** The web is rapidly becoming the go-to environment for deploying and using software. We rely on web technologies to manage our work and social lives, collaborate with like-minded people, experience art and be entertained. Anyone entering the field of computing should have at least a basic understanding of web development, and be able to identify the key opportunities and limitations that web-based software presents. This module focuses on the creation of online interactive experiences. You learn the key languages of web development (HTML5, CSS, JavaScript) - gaining a practical understanding of how they handle content structure/styling and user interactivity. We assume little to no prior experience of web development. You learn from the ground up, working through coding challenges and creative briefs that help embed new techniques and best practice into your programming ‘toolkit’.	
18	**Outline syllabus** ● Hello world (getting started with text editors and HTML5 markup) ● Markup for typesetting ● Image ● Navigation (lists, hyperlinks) ● Video and audio ● Semantic markup ● CSS3 animation (transitions, transformation, keyframing) ● JavaScript for managing interactivity ● Coding conventions and troubleshooting	

- User interfaces and experience design

19 **Teaching and learning activities**

Class Hours

Web Development operates on the principle of ‘learning by making’. Teaching time includes short code demonstrations (to present new techniques), coding challenges, prototyping sessions (to test ideas) and ‘crits’ (to evaluate work). Coding challenges and longer-running projects are undertaken both individually and in small groups.

Independent Learning

In Web Development you encounter several languages that need to work together. This can be daunting at first, but because of the visual nature of HTML5 you soon get to grips with it. Alongside class teaching and assessment preparation we recommend that you set yourself some mini projects to keep your newly acquired knowledge fresh. Ask your tutors for advice on what to attempt.

20 **Intended learning outcomes** *By successful completion of the module, you will be able to demonstrate:*	*How assessed*
1. The application of HTML5 and CSS to create media-rich artefacts that are deployed online.	F1, S2
2. An adherence to coding conventions that ease the review, maintenance and debugging of web applications.	F1, S1, S2
3. The ability to deploy computational thinking to select and apply appropriate technical strategies for addressing a web development problem.	F1, S1, S2
4. The ability to discuss the technical implementation of a web project and reflect critically on the results.	S1, S2

21 **Assessment and feedback**
Formative exercises and tasks:

F1. Code Challenges.

Summative assessments:	*Weighting*
S1. Set exercises.	40%
S2. Web development project. With supporting documentation.	60%

22 **Learning resources**
University Library print and electronic resources, and Minerva:

Key texts:

- Brown, E. (2015). *Learning JavaScript: JavaScript essentials for modern*

	application development (e-book). O'Reilly. ● Duckett, J. (2014) *HTML & CSS: design and build website* (e-book). John Wiley & Sons. ● Sarris, S. (2013). *HTML5 unleashed (e-book).* Sams Publishing. *Key web-based and electronic resources:* ● LinkedIn Learning resources on HTML5, CSS3 and Canvas basics. Accessible via the Bath Spa Library website - https://www.bathspa.ac.uk/library/library-databases ● Periodic table of HTML5 elements - http://websitesetup.org/html5-periodical-table ● Codecademy HTML5/CSS short course - https://www.codecademy.com/learn/web ● Codecademy JavaScript short course - https://www.codecademy.com/learn/learn-javascript *Specialist resources:* ● Brackets Code Editor (cross-platform, free) - http://brackets.io ● Sublime Text Code Editor (cross-platform, free) - http://www.sublimetext.com
23	**Preparatory work** This module requires no previous experience of web development. You may however wish to browse LinkedIn Learning tutorials on the basics of HTML5 for a flavour of what the module covers.

1	Module code	CYS5000-20			
2	Module title	Network Administration			
3	Subject	Cyber Security			
4	Core, Required or Required* for	BSc (Hons) Cyber Security			
5	Level	4	**5**	6	7
6	UK credits	20			
7	ECTS credits	10			
8	Optional for	N/A			
9	Excluded combinations	N/A			
10	Pre-requisite or co-requisite	N/A			
11	Class contact time: total hours	Total Hours: 52			
12	Independent study time: total hours	Total Hours: 148			
13	Semester(s) of delivery	Semester 1			
14	Main campus location	Newton Park			
15	Module co-ordinator	John Curry			
16	Additional costs involved	N/A			

17 **Brief description and aims of module**

This module introduces the technologies and protocols of computer networks. You learn about the core duties of a network administrator, how to build networks using standard devices and interconnect, and how to configure and maintain networks using software tools. Gaining practical experience working with network technologies and architectures is an essential first step towards being able to protect data from unauthorised access. After this module you will be in a better position to identify and address network vulnerabilities, as engage strategies for defending computing systems in modern organisations.

We begin by reviewing the basics of computer network types and typologies, as well as the TCP/IP and OSI (Open Systems Interconnection) reference model. From here you learn best practice for designing, configuring and optimising small-scale computer networks using standard simulation software and physical devices. This begins with a SOHO (small-office-home-office) setup to more complex configurations for larger enterprises. Some key network security controls are also covered in this module, however deeper interaction with this topic is covered later in the programme. The key here is to ensure that you understand computer networking from a practical perspective, including how data is packaged and transported from point A to point B.

18 **Outline syllabus**

- Network types, typologies and services
- The TCP/IP model (Internet Protocol Suite) and OSI reference model
- Configuration of a SOHO network
- IP addressing, subnets and subnetting
- Address Resolution Protocol (ARP)
- Dynamic Host Configuration Protocol (DHCP)
- Domain name system (DNS) and DNSSEC
- Packets, frames and datagrams
- Network commands
- WAN technologies
- Multicasting
- Basic network security controls

19	**Teaching and learning activities** *Class Hours* Lectures introduce core network technologies, typologies, services and protocols. Seminars and workshop activities provide opportunities to configure networks using simulators and physical devices. *Independent Learning* You are expected to follow up recommended readings, as well as extend your understanding of network configuration by engaging simulation and set design activities.	
20	**Intended learning outcomes** *By successful completion of the module, you will be able to demonstrate*	*How assessed*
	1. Knowledge and critical understanding of core network devices and services.	F1, S1
	2. Knowledge and critical understanding of standard network reference models and protocols.	F1, F2, S1, S2
	3. The ability to apply knowledge of networking to configure and troubleshoot a SOHO network.	F2, S2
	4. The ability to critically evaluate the security considerations of a computer network, and apply key threat mitigation techniques.	F2, S1, S2
21	**Assessment and feedback** *Formative exercises and tasks:* F1. In-class quizzes. F2. Network configuration and troubleshooting activities.	
	Summative assessments:	Weighting
	S1. Network design task (2,000 words).	50%
	S2. Networking set exercises.	50%
22	**Learning resources** *University Library print, electronic resources and Minerva:* *Key texts:* ● Stack, E. (2020) *Computer networking beginners guide: a simple and easy guide to manage a network computer system.* Charlie Creative Lab. ● White, M. B. (2018) *Computer networking: the complete guide to understanding wireless technology, network security, computer architecture*	

	and communications systems. CreateSpace. *Key web-based and electronic resources:* ● Cisco Learning Space - https://learningspace.cisco.com ● CompTIA - https://www.comptia.org/resources/computer-networks ● LinkedIn Learning videos and courses on computer networking. Accessible via the Bath Spa Library website - https://www.bathspa.ac.uk/library/library-databases *Specialist resources:* ● Cisco Packet Tracer ● Standard network devices ● Fireeye - https://www.fireeye.com/
23	**Preparatory work** Create a network diagram of your home setup. Show key network devices (e.g. routers, repeaters etc) and typically connected client devices, however do not include IP addresses or any other information that could compromise privacy.

1	Module code	CCO5000-20
2	Module title	CodeLab II
3	Subject	Creative Computing
4	Core, Required or Required* for	BSc (Hons) Creative Computing (Animation) BSc (Hons) Creative Computing (Gaming) BSc (Hons) Creative Computing (Web Technologies) BSc (Hons) Creative Computing Major/Joint/Minor BSc (Hons) Computing BSc (Hons) Cyber Security
5	Level	4 **5** 6 7
6	UK credits	20
7	ECTS credits	10
8	Optional for	N/A
9	Excluded combinations	N/A
10	Pre-requisite or co-requisite	N/A
11	Class contact time: total hours	Total Hours: 52
12	Independent study time: total hours	Total Hours: 148
13	Semester(s) of delivery	Semester 1
14	Main campus location	Newton Park
15	Module co-ordinator	Jake Hobbs
16	Additional costs involved	N/A

17 **Brief description and aims of module**

CodeLab II extends your knowledge of coding to include object-oriented programming (OOP). You build on the procedural programming techniques acquired in CodeLab I to deploy OOP concepts that enhance the functionality and efficiency of your builds.

Beyond developing new technical skills, you learn about the software development cycle. Here you form an understanding of how software projects are planned, implemented and maintained in industry. The ultimate aim of CodeLab II is to develop your programming proficiency to the point where you can independently experiment with unfamiliar coding techniques and languages successfully.

18 **Outline syllabus**

- The software development cycle
- A recap on procedural programming
- Fundamentals of OOP
- Classes and objects
- File handling
- Memory management
- Connecting through Application Programming Interfaces (APIs)
- Graphic user interface (GUI) basics
- Testing and troubleshooting
- Code repositories and version control

19 **Teaching and learning activities**

Class Hours

Learning is predominately lab-based, and evolves through a series of short programming tasks that reinforce understanding of the topics detailed above. Lab sessions also include the introduction of theoretical concepts (usually at the start of sessions) and student-led presentations of individual or collaborative development work. You are required to compile a ‘code repository’ using the web-based service GitHub. The repository is a useful tool for keeping track of specific coding techniques, streamlining your workflow, and to help expedite the software development process.

Independent Learning

Object-oriented programming takes time and effort to understand. You need to establish a routine of review and experimentation to get the most out of CodeLab II and consequently develop your skill set to a good standard. We recommend buddying up with a peer so that you can learn together, collaborate on mini projects and help maintain your motivation. Your tutors provide coding challenges for you to undertake during independent study, as well as point to LinkedIn Learning resources to support your learning.

20	**Intended learning outcomes** *By successful completion of the module, you will be able to demonstrate*	*How assessed*
	1. The implementation and testing of a prototype system that is driven by object-oriented programming techniques.	F2, S1, S2
	2. Application of the iterative design cycle of prototyping, testing, analysing and refinement.	F2, S1, S2
	3. A recognition of personal knowledge limits, which is addressed through the identification of learning opportunities.	F1, F2, S2
	4. The ability to critically review the key features and challenges of developing software for an end user, and evaluate their relevance to the field of creative computing.	F2, S2

21 **Assessment and feedback**

Formative exercises and tasks:

F1. Skills Test. Conducted at the beginning of the module.

F2. Project Reviews.

Summative assessments:	Weighting
S1. Programming skills portfolio.	40%
S2. Data-driven application. With supporting documentation.	60%

22 **Learning resources**

University Library print, electronic resources and Minerva:

Key Texts:

- Denning, P. J. & Tedre, M. (2019) *Computational thinking.* MIT Press
- Leach, R. J. (2016). *Introduction to software engineering* (ebook). Chapman & Hall.
- Meyers, S. (2015). *Effective modern C++* (e-book). O'Reilly.
- Murray, A. P. (2016). *The complete software project manager* (e-book). John Wiley & Sons.
- Savitch, W. (2016). *Absolute C++, global edition* (e-book). Pearson Education.
- Stroustrup, B. (2014). *Programming: principles and practice using C++.* Addison-Wesley.

Key web-based and electronic resources:

- LinkedIn Learning resources related to object-oriented programming. Accessible via the Bath Spa Library website - https://www.bathspa.ac.uk/library/library-databases

Specialist resources:

- Github, web based code repository & version control – http://github.com
- Github Desktop, version control tool – http://desktop.github.com
- Visual Studio – https://www.visualstudio.com
- XCode – https://developer.apple.com/xcode

23 **Preparatory work**

You should ensure that you are familiar with the procedural programming techniques introduced in CodeLab I before undertaking this module.

1	Module code	CPU5002-20			
2	Module title	Databases			
3	Subject	Computing			
4	Core, Required or Required* for	BSc (Hons) Computing BSc (Hons) Cyber Security			
5	Level	4	**5**	6	7
6	UK credits	20			
7	ECTS credits	10			
8	Optional for	N/A			
9	Excluded combinations	N/A			
10	Pre-requisite or co-requisite	N/A			
11	Class contact time: total hours	Total Hours: 52			
12	Independent study time: total hours	Total Hours: 148			
13	Semester(s) of delivery	Semester 1			
14	Main campus location	Newton Park			
15	Module co-ordinator	Dave Cobb			
16	Additional costs involved	N/A			

17 **Brief description and aims of module**

This module provides an introduction to the design, creation and use of databases. It exposes particularly the function of relational databases, and the various data modelling approaches required to create solutions that are organised efficiently, robust and appropriately secure.

The aim of *Databases* is to provide practical experience of implementing applications that leverage standard relational database management systems (RDBMS). You learn how to determine appropriate relationships between data entities and how to represent them, use SQL notation to retrieve and manipulate data, and deploy database normalisation forms to ensure data integrity. During the module we utilise variants of the LAMP web service stack, deploying MySQL and PHP to negotiate transactions with databases and serve content to users via web browsers. Module content therefore also incorporates aspects of HTML markup and JavaScript scripting to develop simple, yet focused dynamic web applications.

18 **Outline syllabus**

- The function and scope of databases within computing
- An overview of relational database management systems (RDBMS)
- Interpreting Requirements Specification documents
- Expressing data relationships via an entity-relationship (ER) diagram
- Data modelling – conceptual, logical and physical models
- Normalisation
- Implementing and querying databases
- Approaches to serving content to users
- Data security best practices - data classifications, risks and controls

19 **Teaching and learning activities**

Class Hours

The module includes a lecture component that introduces underlying concepts and principles, and supporting lab sessions to allow for application of specific tools and techniques. A series of database modelling, implementation and querying tasks are undertaken to audition the skills required to complete summative assessments.

Independent Learning

It is recommended that you develop an appropriate workflow on a personal computer to enable you to enhance your understanding of database design and implementation outside of class hours.

20	**Intended learning outcomes** *By successful completion of the module, you will be able to demonstrate:*	*How assessed*
	1. The ability to implement a database design that addresses a defined requirement specification.	F1, S1, S2
	2. Knowledge and critical understanding of data modelling approaches, and the formal methods used to express relationships between entities.	F1, S1, S2
	3. The ability to select and implement tools and procedures for querying and manipulating databases, and serving content to a user.	F2, S2
	4. Critical understanding of database management issues, and the ability to mitigate them.	S2

21	**Assessment and feedback** *Formative exercises and tasks:*	
	F1. Database modelling exercises.	
	F2. Querying tasks.	
	Summative assessments:	Weighting
	S1. Database model with annotations.	30%
	S2. Web application. With supporting documentation.	70%

22 **Learning resources**

University Library print, electronic resources and Minerva:

Key texts:

- Hammer, M. (2017) *Relational database practices: bridging the gap between theory of database design and real-world practices.* Malcolm Hamer.
- Hernandez, M. (2013) *Database design for mere mortals: a hands-on guide to relational database design.* Addison-Wesley Professional.

Key web-based and electronic resources:

	● Codecademy PHP and SQL (interactive tutorials) – Available at https://www.codecademy.com ● Library of database models – http://www.databaseanswers.org/data_models/index.htm ● LinkedIn Learning courses related to SQL, PHP and JavaScript. Accessible via the Bath Spa Library website - https://www.bathspa.ac.uk/library/library-databases
23	**Preparatory work** Review the ‘Library of database models’ website listed above to become familiar with the range of ways that data relationships can be represented. A working knowledge of HTML and JavaScript is required for this module. It is also highly recommended that you use Codecademy interactive tutorials to ensure that you are comfortable with the fundamentals of both languages.

1	Module code	CYS5001-20			
2	Module title	Intrusion Analysis and Response			
3	Subject	Cyber Security			
4	Core, Required or Required* for	BSc (Hons) Cyber Security			
5	Level	4	**5**	6	7
6	UK credits	20			
7	ECTS credits	10			
8	Optional for	N/A			
9	Excluded combinations	N/A			
10	Pre-requisite or co-requisite	N/A			
11	Class contact time: total hours	Total Hours: 52			
12	Independent study time: total hours	Total Hours: 148			
13	Semester(s) of delivery	Semester 2			
14	Main campus location	Newton Park			
15	Module co-ordinator	John Curry			
16	Additional costs involved	N/A			

17 **Brief description and aims of module**

Knowing when the confidentiality, integrity or availability of an enterprise computer system has been compromised is critical for business continuity. Understanding how to confirm a breach and respond accordingly to minimise impact and expedite a return to normal working practices is essential for the cyber security practitioner.

Intrusion Analysis and Response aims to help you develop the specialised technical knowledge needed to identify and act on potential network intrusions. We begin with a review of several types of network breach, how they are conducted, and their potential effects on business continuity. Next, we critically examine systems for detecting and preventing intrusions, including what network traffic they observe, what rules they use to flag unexpected activity, and what actions they take to eliminate threats. We then turn to incident analysis and response. Here you compare published guidance from the public and private sector, and apply methods for intrusion containment, restoring operations and improving security posture via post-incident analysis.

18 **Outline syllabus**

- The top 10 current network attacks
- Physical security: reducing the risk of on-site attacks
- The types, operation, and trade-offs of intrusion detection systems (IDS) and intrusion prevention systems (IPS)
- Signature, anomaly and behaviour-based detection methods
- Filtering and investigating activity alerts
- Incident response plans and protocol
- The NIST (National Institute of Standards and Technology) incident response lifecycle and alternative incident response guidance
- NCSC (National Cyber Security Centre) Incident Management guidance
- Containment strategies (segmentation, isolation, removal)
- Restoring operations: eradication and recovery activities
- Remediating vulnerabilities and enhancing security controls
- Media sanitisation techniques
- Post-incident review and incident reporting

19	**Teaching and learning activities** *Class Hours* Classes are predominately workshop based, allowing time to engage technologies and strategies for detecting and resolving network intrusions. Workshops are contextualised with seminar segments where concepts, published frameworks and best practice is critically examined. *Independent Learning* You are expected to undertake readings set by tutors, as well as deepen your understanding of intrusion detection/prevention and response by analysing relevant case studies.	
20	**Intended learning outcomes** *By successful completion of the module, you will be able to demonstrate*	*How assessed*
	1. Knowledge and critical understanding of established methods for intrusion detection and prevention.	F1, S1
	2. The ability to apply specialist tools to collect and analyse unusual behaviour on a network.	F1, S1
	3. The ability to apply established frameworks for incident response to generate solutions for containing and eradicating threats to a network.	F1, S1, S2
	4. The ability to formulate and justify recommendations for improving network security post-incident.	F2, S2
21	**Assessment and feedback** *Formative exercises and tasks:* F1. Intrusion analysis and response set exercises. F2. Lessons learnt roundtable.	
	Summative assessments:	Weighting
	S1. Network intrusion analysis (3,000 words).	60%
	S2. Post-incident report (2,000 words)	40%
22	**Learning resources** *University Library print, electronic resources and Minerva:* *Key texts:* ● Johansen, G. (2020) *Digital forensics and incident response: a practical guide to deploying digital forensic techniques in response to cyber security incidents.* Packt Publishing.	

	● Mukherjee, A. (2020) *Network security strategies: protect your network and enterprise against advanced cybersecurity attacks and threats.* Packt Publishing. *Key web-based and electronic resources:* ● NIST Computer Security Incident Handling Guide (2012) ● SANS Incident Handling Process for Small and Medium Businesses ● NCSC incident management guidance - https://www.ncsc.gov.uk/collection/incident-management ● LinkedIn Learning videos and courses related to intrusion analysis and response. Accessible via the Bath Spa Library website - https://www.bathspa.ac.uk/library/library-databases *Specialist resources:* ● Wireshark (network protocol analyser) - https://www.wireshark.org ● SolarWinds Security Event Manager - https://www.solarwinds.com/security-event-manager ● SNORT (open source IPS) - https://www.snort.org
23	**Preparatory work** Conduct some preliminary research online on the function of an intrusion detection/prevention system as well as the steps recommended by NIST to respond to a network intrusion.

1	Module code	CYS5002-20			
2	Module title	Cyber Resilience			
3	Subject	Cyber Security			
4	Core, Required or Required* for	BSc (Hons) Cyber Security			
5	Level	4	**5**	6	7
6	UK credits	20			
7	ECTS credits	10			
8	Optional for	N/A			
9	Excluded combinations	N/A			
10	Pre-requisite or co-requisite	N/A			
11	Class contact time: total hours	Total Hours: 52			
12	Independent study time: total hours	Total Hours: 148			
13	Semester(s) of delivery	Semester 2			
14	Main campus location	Newton Park			
15	Module co-ordinator	John Curry			
16	Additional costs involved	N/A			

17 **Brief description and aims of module**

Cyber criminals are adapting faster than security solutions are being devised. Many specialists agree that traditional cyber security measures are proving inadequate at handing the persistence and complexity of the evolving threat landscape. The concept of cyber resilience in turn represents a shift in mindset to one that assumes that cyber attacks are inevitable, and that organisations should focus efforts on developing post-breach strategies in addition to mitigatory measures. Cyber resilience is about an organisation's ability to reduce the impact of an attack, and it's capacity to return to operations as quickly as possible.

We begin with a review of the subtle yet critical differences between cyber security and cyber resilience with a particular focus on the notion of 'assuming breach'. We then consider what cyber resilience means for the public, private and third sector, which includes an understanding of relevant published frameworks from the UK and other global powers. This is followed by a deep examination of potential strategies that an organisation can put in place for improving cyber resilience. This includes planning decisions that target cost of attack and risk exposure, as well as ways that organisations fine tune their post-incident recovery plans to meet individual circumstances.

18 **Outline syllabus**

- Cyber security vs cyber resilience
- The scope of cyber resilience: organisations, critical infrastructure, society, nation states
- Assuming breach: taking on an adversary mindset
- IT Governance Cyber Resilience Framework
- MITRE ATT&CK framework
- Defining a bespoke and robust organisational cyber resilience strategy
- Identifying cyber risk (pure and speculative) and its place within business risk management
- Analysing and calculating risk exposure
- The problem of security decay and cyber hygiene
- Tensions between security and complexity

- Cyber resilience through compliance: GDPR, Cyber Essentials and related ISO (International Organization for Standardization) standards
- The importance of organisational collaboration

19 **Teaching and learning activities**

Class Hours

Lectures and seminars are highly focused on strategic thinking and case study analysis. This is support where possible from insights on specific cyber resilience strategies from invited speakers. Workshop sessions invite you to establish and critically evaluate threat mitigation and post-incident recovery solutions for hypothetical business contexts.

Independent Learning

You are expected to undertake readings set by tutors and follow up concepts and examples introduced in class through independent research.

20	**Intended learning outcomes** *By successful completion of the module, you will be able to demonstrate*	*How assessed*
	1. Knowledge and critical understanding of the relationship between cyber security and cyber resilience in terms of objectives and guiding principles.	F1, F2, S1
	2. The ability to critically evaluate the cyber resilience strategy of an organisation.	F1, F2, S1
	3. The ability to critically evaluate and apply published guidance and standards to make recommendations for improving the cyber resilience of an organisation.	F2, S1
	4. Critical awareness of the value and application of collaborative practice in establishing best practice for organisational cyber resilience.	F2, S1
	Assessment and feedback *Formative exercises and tasks:* F1. Case study analysis. F2. Cyber resilience plan submission and review milestones.	
	Summative assessments:	Weighting
	S1. Cyber resilience plan (5,000 words).	100%

21 **Learning resources**

University Library print, electronic resources and Minerva:

Key texts:

	● Calder, A. (2020) *The cyber security handbook: prepare for, respond to and recover from cyber attacks with the IT Governance Cyber Resilience Framework.* IT Governance Publishing. ● Petrenko, S. (2019) *Cyber resilience.* River Publishers. ● Zongo, P. (2018) *The five anchors of cyber resilience: why some enterprises are hacked into bankruptcy while others easily bounce back.* CISO Advisory. *Key web-based and electronic resources:* ● IT Governance cyber resilience resources - https://www.itgovernance.co.uk/resources/cyber-resilience ● GDPR - https://gdpr-info.eu ● National Cyber Security Centre - https://www.ncsc.gov.uk ● Cyber Essentials - https://www.ncsc.gov.uk/cyberessentials/overview ● Cyber Resilience Toolkit (Scottish Government) and related resources - https://www.gov.scot/
22	**Preparatory work** Read the materials on cyber resilience published by IT Governance.

1	Module code	CPU5003-20
2	Module title	Software Project Management
3	Subject	Computing
4	Core, Required or Required* for	BSc (Hons) Computing
5	Level	4 **5** 6 7
6	UK credits	20
7	ECTS credits	10
8	Optional for	BSc (Hons) Cyber Security
9	Excluded combinations	N/A
10	Pre-requisite or co-requisite	N/A
11	Class contact time: total hours	Total Hours: 52
12	Independent study time: total hours	Total Hours: 148
13	Semester(s) of delivery	Semester 2
14	Main campus location	Newton Park
15	Module co-ordinator	Dave Cobb
16	Additional costs involved	N/A

17 **Brief description and aims of module**

Software project management refers to industry standard techniques used to develop and deliver various types of software products. It includes aspects such as how to choose appropriate software development methodologies and technologies, estimate project size and build schedule, allocate resources effectively and uphold a safe working environment.

This module introduces the fundamental skills required to manage the development of software products. You learn how to produce a project management plan, define organisation roles, allocate resources, select appropriate development methodologies, and monitor and report on progress. Scheduling and costing also factors into this module, as does identifying and managing risk. *Software Project Management* in addition identifies and evaluates a range of tools for task allocation and tracking, as well as code review and versioning. You gain practical experience with these tools via a compressed collaborative development exercise.

18 **Outline syllabus**

- The role of the software project manager
- The project management lifecycle
- Software development methodologies and workflows - from traditional predictive approaches through agile and DevOps
- Identifying and deploying tools for task allocation, collaborative working, code review and versioning
- Quality assurance practices
- Risk management
- Reporting methods

19 **Teaching and learning activities**

Class Hours

Activities in session comprise both theory and practice-led sessions. Lectures cover theories related to software project management with reference to industry standard

	practices. Seminar sessions evaluate historical scenarios where companies have deployed software project management strategies effectively (and otherwise), while workshop sessions provide practical experience of using task allocation and tracking tools, as well as platforms for collaborative development. *Independent Learning* Part of this module requires you to develop a piece of software in collaboration with peers. You are expected to schedule time for both remote working and team meetings, and maintain commitment when working with others. Similarly, it is important to allocate appropriate time each week to engaging the summative assessment, *Virtual Project.* This assessment is longitudinal in approach, requiring you to address emerging challenges and opportunities as they are introduced.	
20	**Intended learning outcomes** *By successful completion of the module, you will be able to demonstrate:*	*How assessed*
	1. The ability to discuss critically the role of a software project manager, including their responsibilities and challenges.	F1, S2
	2. Knowledge of underlying software project management strategies used in industry, and the critical evaluation and selection of appropriate related methods to address a defined task.	F1, F2, S1, S2
	3. Critical understanding of requirements management, quality assurance and risk mitigation processes in the context of software project management.	F1, S2
	4. The application of tools and methods that support collaboration and communication with stakeholders of a software development project.	F2, S1
21	**Assessment and feedback** *Formative exercises and tasks:* F1. Project reporting (presentations). F2. Supervised team meetings.	
	Summative assessments:	Weighting
	S1. Presentation. On the collaborative development exercise. (20 minutes, group).	40%
	S2. Virtual project (3,000 words).	60%
22	**Learning resources** *University Library print, electronic resources and Minerva:* *Key texts:*	

	● Bennet, L. (2017) *Managing successful projects with PRINCE2.* Stationery Office. ● Cole, R. & Scotcher, E. (2015) *Brilliant Agile project management: a practical guide to using Agile, Scrum and Kanban.* Pearson Business. ● Galin, D. (2018) *Software quality: concepts and practice.* Wiley-Blackwell. ● Gleeson, P (2017) *Working with coders: a guide to software development for the perplexed non-techie.* Apress. ● Hinde, D. (2016) *The project manager and the pyramid: how to manage any project, any place, any time.* Orgtopia. ● Sutherland, J. (2015) *Scrum: the art of doing twice the work in half the time.* Random House Business. ● Harrison, D. & Lively, K. (2019) *Achieving DevOps*. Apress. *Key web-based and electronic resources:* ● GitHub – https://github.com ● LinkedIn Learning courses related to project management and development strategies. Accessible via the Bath Spa Library website - https://www.bathspa.ac.uk/library/library-databases ● Various software project management tools – introduced in class.
23	**Preparatory work** Ensure that you are comfortable with using GitHub.

1	Module code	CCO5103-20
2	Module title	The Responsive Web
3	Subject field	Creative Computing
4	Core, Required or Required* for	BSc (Hons) Creative Computing (Web Technologies)
5	Level	5
6	UK credits	20
7	ECTS credits	10
8	Core, Required, Required* or Optional	Required/Optional
9	Optional for	BSc (Hons) Creative Computing Major BSc (Hons) Computing
10	Excluded combinations	N/A
11	Pre-requisites and co-requisites	Web Development
12	Class contact time: total hours	Total Hours: 52
13	Independent study time: total hours	Total Hours: 148
14	Semester(s) of delivery	Semester 2
15	Main campus location	Newton Park
16	Module co-ordinator	Gary Renes
17	Additional costs involved	None
18	Brief description and aims of module The Responsive Web builds on the HTML5, CSS and JavaScript programming skills covered in Web Development. Following a HTML5 refresher, you be introduced to frameworks and layout modules (e.g. Flexbox and CSS Grid) that help implement responsive web design. You then encounter CSS animation and JavaScript techniques to manage user events. Beyond the technical aspects of the module you are taught strategies to test and troubleshoot your web development projects. These include in part, the utilisation of Chrome Development Tools and various web services that help improve accessibility, search engine optimisation (SEO) and markup validation.	
19	Outline syllabus Topics covered in The Responsive Web include: • HTML5, CSS and JavaScript refresher • Introduction to responsive web design (RWD) • Media Queries, Flexbox and CSS Grid • The HTML Document Object Model (DOM) • JavaScript for event handing • CSS animation • Testing and troubleshooting strategies • Markup validation • Accessibility and search engine optimisation (SEO)	
20	Teaching and learning activities *Class Hours* Learning is predominately lab-based, and evolves through a series of short programming tasks that reinforce understanding of the topics listed above. Lab sessions include the introduction of theoretical concepts and student-led	

	presentations of development work. You are advised strongly to compile a ‘code repository’ locally or on a web-based service such as GitHub. The repository is a useful tool for keeping track of specific coding techniques and streamlining your workflow. *Independent Learning* Independent study helps consolidate and extend your lab-based learning. Short research and development tasks are set regularly to aid your review of in-class material and support your understanding of HTML5, CSS3 and JavaScript techniques. Often these exercises encourage collaboration with one or more learning partners. You are provided with a bank of learning resources via Minerva that comprise tutor presentations (with notes), code snippets and links to LinkedIn Learning video tutorials. It is good practice to get into a routine of exploring these materials, giving yourself enough time to follow up on topics that particularly interest you or require further clarification.	
21	Intended learning outcomes *By successful completion of the module, you will be able to demonstrate:*	*How assessed*
	• The application of HTML5, CSS and JavaScript to deliver responsive layouts that target key device types and resolutions.	S1, S2
	• An ability to implement web applications that conform to contemporary web design conventions (semantic markup, accessibility, SEO).	S1, S2
	• Successful deployment of a range of strategies for testing, troubleshooting and debugging web projects that exploit responsive layouts.	F1, S1, S2
	• An ability to document the successes/limitations of an original build and identify personal learning opportunities for improving web development skills.	F1, S2
22	Assessment and feedback *Formative exercises and tasks:* F1. Web Refresher.	
	Summative assessments:	*Weighting*
	S1. Clone Tasks.	50%
	S2. Multi-Device Application. Supported by a 1000 word development document.	50%
23	Learning resources *University Library print and electronic resources, and Minerva:* *Key texts:* • Brown, E. (2015). *Learning JavaScript: JavaScript essentials for modern application development* (e-book). O’Reilly. • Clark, J. (2015). *Responsive web design in practice* (e-book). Rowman &	

	Littlefield. • Firdaus, T. (2016). *HTML5 and CSS3: building responsive websites: design robust, powerful, and above all, modern websites across all manner of devices with ease using HTML5 and CSS3: a course in three modules* (e-book). Packt Publishing. • Reiss, E. (2012). *Usable usability* (e-book). John Wiley & Sons. *Key web-based and electronic resources:* • LinkedIn Learning resources related to HTML5, JavaScript and CSS. Links shared in class. • Codecademy courses on HTML5, JavaScript and CSS - https://www.codecademy.com/ *Specialist resources:* • Coda Development Environment (Mac) - https://panic.com/coda/ • Brackets Code Editor (Mac, free) - http://brackets.io/ • Sublime Text Code Editor (cross-platform, free) - http://www.sublimetext.com/ • Cross-browser testing - https://www.browserling.com/ • Website Rating (code quality, linking, semantic markup) - http://nibbler.silktide.com/ • Koala SCSS Compilation Tool - http://koala-app.com/
24	Preparatory work Students undertaking The Responsive Web would benefit greatly from a HTML5 refresher. A good short course is offered by Codecademy https://www.codecademy.com/learn/web (est. 4 hours).

1	Module code	PPY5100-120			
2	Module title	Professional Placement Year			
3	Subject	All four year courses with Professional Placement Year			
4	Core, Required or Required* for	N/A			
5	Level	4	**5**	6	7
6	UK credits	120			
7	ECTS credits	60			
8	Optional for	All			
9	Excluded combinations	N/A			
10	Pre-requisite or co-requisite	N/A			
11	Class contact time: total hours	Minimum hours of support: 10			
12	Independent study time: total hours	Total Hours: 1190			
13	Semester(s) of delivery	1 academic year			
14	Main campus location	N/A			
15	Module co-ordinator	Individual course/subject leader or nominee			
16	Additional costs involved	Additional costs will depend on the nature and location of placement			

17 **Brief description and aims of module**

Structured work placements are considered to be a key determinant in gaining graduate level employment on graduation by both employers and students. This module provides you with the opportunity to identify, apply for, and secure professional experience, normally comprising 1-3 placements over a minimum of 9 months, which attracts 120 Level 5 credits. By completing the module, you will be entitled to the addition of “with Professional Placement Year” to your degree title; evidencing your work and success in respect of your placement, and demonstrating your ability to secure and sustain graduate-level employment.

By taking part in this module, you will be addressing the following graduate attributes:

- Employable: equipped with the skills necessary to flourish in the global workplace, able to work in, and lead, teams.
- Able to understand and manage complexity, diversity and change.
- Creative, able to innovate and to solve problems by working across disciplines as professional or artistic practitioners.
- Creative thinkers, doers and makers.

18 **Outline syllabus**

Before/at the start of your sandwich year, you will work on your development plan with the Module Leader and your placement coordinator from the Careers and Employability team. This development plan asks you to provide details of up to four development themes that you develop and measure during your placement. This is marked at the beginning of your placement. At the very start of your return to university for your final year, you will submit your Placement Portfolio, detailing your development on placement.

Prior to commencing your sandwich year placement(s), you will need to complete all relevant Placement forms. Throughout your placement(s) you will need to ensure you adhere to the requirements of the University's Work Placement Policy.

19 **Teaching and learning activities**

In preparation for the actual placement, support will be available from the Careers and Employability team in your first and second year of study.

Once you have secured a placement, you will be supported through tutorials, both face to face and remotely, to prepare you for your placement and the assessment requirements of this module. Your development plan will be agreed and assessed early in your placement.

While on placement, you will be supported by a placement supervisor in work, the Module Leader and the placement coordinator from the Careers and Employability team. You will have supervisory communication with the module leader or placement coordinator at least once a month throughout your sandwich year. This will also support completion of the second assessment item.

20	**Intended learning outcomes** *By successful completion of the module, you will be able to demonstrate:*	*How assessed*
	1. Critically evaluate the learning opportunities provided in the workplace and reflect on the personal growth and development gained through the successful completion of your placement.	F1, S1, S2
	2. Communicate effectively and appropriately to a range of audiences.	F1, S1, S2
21	**Assessment and feedback** *Formative exercises and tasks:*	
	F1. Reflective log.	
	Summative assessments:	Weighting
	S1. Development plan (equivalent to 1,500 words)	Pass/fail only
	S2. Placement portfolio (equivalent to 3,500 words)	Pass/fail only

22 **Learning resources**
University Library print, electronic resources and Minerva:

Key texts:

- Bolton, G., (2010) *Reflective Practice: Writing and Professional Development.* London: Sage Publications.
- Fanthome, C., (2004) *Work Placements: A Survival Guide for Students*, London: Palgrave Macmillan.
- Herbert, I., Rothwell, A., (2004), *Managing Your Placement: A Skills-Based Approach*, Hampshire, Palgrave MacMillan
- Sweitzer, H. F., and King, M. A., (2014) *The successful internship: personal,*

	professional and civic development in experiential learning, Cengage. *Key web-based and electronic resources:* ● National Council for Work experience, http://www.work-experience.org/ncwe.rd/index.jsp ● Grad South West – http://www.gradsouthwest.com ● Tool Kits for Success - http://www.disabilitytoolkits.ac.uk/students/before.asp ● Business Source Complete, Newsbank and Mintel (accessible through the library) ● Bath Spa CareerHub (http://www.careerhub.bathspa.ac.uk) ● National Council for Work Experience (http://www.work-experience.org) ● Prospects: Work Experience and Internships (http://www.prospects.ac.uk/work_experience.htm)
23	**Preparatory work** You will need to find and secure your placement(s) in advance of this module.

<table>
<tr><td>1</td><td>Module code</td><td colspan="4">CYS6000-20</td></tr>
<tr><td>2</td><td>Module title</td><td colspan="4">Cyber Crime, Law and Ethics</td></tr>
<tr><td>3</td><td>Subject</td><td colspan="4">Cyber Security</td></tr>
<tr><td>4</td><td>Core, Required or Required* for</td><td colspan="4">BSc (Hons) Cyber Security</td></tr>
<tr><td>5</td><td>Level</td><td>4</td><td>5</td><td><b>6</b></td><td>7</td></tr>
<tr><td>6</td><td>UK credits</td><td colspan="4">20</td></tr>
<tr><td>7</td><td>ECTS credits</td><td colspan="4">10</td></tr>
<tr><td>8</td><td>Optional for</td><td colspan="4">N/A</td></tr>
<tr><td>9</td><td>Excluded combinations</td><td colspan="4">N/A</td></tr>
<tr><td>10</td><td>Pre-requisite or co-requisite</td><td colspan="4">N/A</td></tr>
<tr><td>11</td><td>Class contact time: total hours</td><td colspan="4">Total Hours: 39</td></tr>
<tr><td>12</td><td>Independent study time: total hours</td><td colspan="4">Total Hours: 161</td></tr>
<tr><td>13</td><td>Semester(s) of delivery</td><td colspan="4">Semester 1</td></tr>
<tr><td>14</td><td>Main campus location</td><td colspan="4">Newton Park</td></tr>
<tr><td>15</td><td>Module co-ordinator</td><td colspan="4">John Curry</td></tr>
<tr><td>16</td><td>Additional costs involved</td><td colspan="4">N/A</td></tr>
</table>

17 **Brief description and aims of module**

Cyber crime is an expansive and growing problem, perpetrated by cyber criminals and state-sponsored actors, and enabled by the same technologies that underpin the world economy and our daily lives. This module covers the primary types of cyber crime, including those related to personal or financial gain, and those which compromise the confidentiality, integrity, and availability of information.

In *Cyber Crime, Law and Ethics* you explore the laws and legal protections in place in the UK and internationally, and how they have developed in response to the increasing threat to privacy, security and intellectual property. You critically evaluate the complex relationship between privacy and security, and the ongoing ethical challenges to personal freedoms in the interests of the greater good.

18 **Outline syllabus**

- Types of threat actor, cyber crime, and their effects
- Key UK and international legislation
- Issues in applying and updating cyber crime law
- Core ethical challenges in cyber security
- The relationship between cyber security and civil liberty
- The ethical implications of security strategies that rely on Artificial Intelligence or other imperfect tools
- Upholding professionalism and integrity
- Transparency and responsible disclosure
- Emerging challenges in cyber law and ethics

19 **Teaching and learning activities**

Class Hours

Seminar sessions are discursive, with a strong emphasis on individual and group research. Detail on the evolution and application of law are supported by guest speakers where appropriate.

	Independent Learning You are expected to lend significant time to investigating the concepts and issues introduced in class. You should also ensure that you diligently document your findings and analyses as elements to include in your assessment portfolio, as well as for tutor review.	
20	**Intended learning outcomes** *By successful completion of the module, you will be able to demonstrate*	*How assessed*
	1. Systematic knowledge of common forms of cyber crime and how such crimes are perpetrated.	F1, S1, S2
	2. A systematic understanding of ethical challenges in cyber security and the responsibilities of sector professionals.	F1, F2, S2
	3. The ability to synthesise information from a range of sources in order to establish a critical position on the relationship between cyber security and civil liberty.	F1, F2, S2
	4. The ability to devise arguments on the legal and ethical implications of computer use.	F1, F2, S1, S2
21	**Assessment and feedback** *Formative exercises and tasks:* F1. Case study analysis. F2. Debate. On ethical issues surrounding security and privacy.	
	Summative assessments:	Weighting
	S1. Cyber crime visualisation. With supporting annotations.	30%
	S2. Case study portfolio (3,500 words).	70%
22	**Learning resources** *University Library print, electronic resources and Minerva:* *Key texts:* ● Gillespie, A. A. (2019) *Cybercrime: key issues and debates.* Routledge. ● Kosseff, J. (2019) *Cybersecurity law*. Wiley. ● Manjikian, M. (2017) *Cybersecurity ethics: an introduction.* Routledge. ● Sutton, D. (2017). *Cyber security: a practitioner's guide*. BCS Learning & Development Limited. ● Yar, M. and Steinmetz, K. F. (2019) *Cybercrime and society.* SAGE Publications. *Key web-based and electronic resources:*	

	● Christen, M., Gordijn, B. and Loi, M. (2020) *The ethics of cybersecurity.* Springer. Open access text available at https://www.researchgate.net/publication/339161649_The_Ethics_of_Cybersecurity ● Crown Prosecution Service resources on cyber crime - https://www.cps.gov.uk/crime-info/cyber-online-crime ● International Comparative Legal Guides resources on cyber law and regulation - https://iclg.com/practice-areas/cybersecurity-laws-and-regulations ● The National Cyber Security Centre - https://www.ncsc.gov.uk ● ACM Transactions on Privacy and Security (TOPS) - https://dl.acm.org/journal/tops
23	**Preparatory work** Use online sources to Identify a case of cyber crime, and determine (to the best of your ability at this early stage in the module) what laws and/or ethics standards may have been compromised.

1	Module code	CYS6001-20			
2	Module title	Research Project			
3	Subject	Cyber Security			
4	Core, Required or Required* for	BSc (Hons) Cyber Security			
5	Level	4	5	**6**	7
6	UK credits	20			
7	ECTS credits	10			
8	Optional for	N/A			
9	Excluded combinations	N/A			
10	Pre-requisite or co-requisite	N/A			
11	Class contact time: total hours	Total Hours: 39			
12	Independent study time: total hours	Total Hours: 161			
13	Semester(s) of delivery	Semester 1			
14	Main campus location	Newton Park			
15	Module co-ordinator	John Curry			
16	Additional costs involved	N/A			

17 **Brief description and aims of module**

This module provides an opportunity to investigate an area of cyber security of personal interest, and ideally one that engages a professional role that you wish to pursue. The core aim is to identify and critically evaluate current knowledge in the field with a view to developing cogent arguments and insights on that topic. This may include data collection exercises, or otherwise be conducted as a desk-based research activity.

You begin by identifying several potential areas of investigation and consulting with your project supervisor to agree on a single topic of enquiry. Following drafting of a research question, you draw on self-selected readings to conduct a literature review and consolidate resulting insights using a literature review map. Supported by lectures on research methods and knowledge exchange seminars, you then undertake further readings and/or conduct data collection activities independently to construct a critical argument on your chosen topic. Finally, you structure and write-up an academic paper that presents your findings.

18 **Outline syllabus**

- Planning and managing a self-directed research project
- Identifying a topic of enquiry
- Setting aims and objects
- Ethical considerations and approval mechanisms
- Developing a clear research proposal
- Research methods in the field of cyber security
- Academic writing and review

19 **Teaching and learning activities**

Class Hours

Lecturers provide critical insight into research methods in the field of cyber security while seminars offer an opportunity to share and discuss emerging insights with peers.

	Independent Learning Conducting a research project requires a significant commitment to self-directed academic study. You must be organised, motivated, inquisitive and prepared to adjust your direction/perspectives in response to emerging insights. It is critical also that you engage your project supervisor regularly to help support your trajectory through the research.	
20	**Intended learning outcomes** *By successful completion of the module, you will be able to demonstrate*	*How assessed*
	1. Systematic knowledge of an area of cyber security, including that which exists at the forefront of the discipline.	F2, S2
	2. The ability to critically evaluate, interpret and synthesise data from a variety of sources as required to develop cogent insights into an area of cyber security.	F2, S1, S2
	3. Critical evaluation, adaptation and application of research methods as required to address a self-devised question in the field of cyber security.	F1, S2
	4. The ability to devise, sustain and communicate arguments on a self-selected topic in the field of cyber security.	F1, S1, S2
21	**Assessment and feedback** *Formative exercises and tasks:* F1. Research proposal. F2. Literature review map.	
	Summative assessments:	Weighting
	S1. Lightning talk (5 minutes).	20%
	S2. Research paper (4,000 words).	80%
22	**Learning resources** *University Library print, electronic resources and Minerva:* *Key texts:* ● Chatfield, T. (2018) *Critical thinking: your guide to effective argument, successful analysis and independent study*. Sage Publications Ltd. ● Creswell, J. (2018) *Research design: qualitative, quantitative, and mixed methods approaches*. Sage Publications. ● Greetham B. (2019) *How to Write Your Undergraduate Dissertation* (Macmillan Study Skills). ● Landau-Pope, J. (2017) *What's your excuse for not being more productive?: overcome your excuses, stop procrastinating, get things done*. WYE	

	Publishing. *Specialist resources:* Specialist resources required to meet the objectives of your dissertation should be discussed individually with your project supervisor.
23	**Preparatory work** Consider three potential topics for your research project and a bullet point list of pros and cons for each.

1	Module code	CYS6002-20
2	Module title	Securing the Internet of Things
3	Subject	Cyber Security
4	Core, Required or Required* for	N/A
5	Level	4 5 **6** 7
6	UK credits	20
7	ECTS credits	10
8	Optional for	BSc (Hons) Cyber Security
9	Excluded combinations	N/A
10	Pre-requisite or co-requisite	N/A
11	Class contact time: total hours	Total Hours: 39
12	Independent study time: total hours	Total Hours: 161
13	Semester(s) of delivery	Semester 1
14	Main campus location	Newton Park
15	Module co-ordinator	John Curry
16	Additional costs involved	N/A

17 **Brief description and aims of module**

The Internet of Things (IoT) is a potentially game changing technology that enables myriad devices to be connected and monitored continuously via the Internet. This enhanced connectivity has led to fascinating innovations such as autonomous vehicles, home automation, enhanced energy management, health monitoring and tools for improving business productivity, as well as many applications that have not yet been considered. IoT has been adopted quickly across almost all industries and domains with the objective of lessening the burden on humans.

As reliance on IoT grows, malicious hacker groups are choosing to target smart systems for cyber attack. This has implications for both organisations and citizens in terms of privacy, financial loss, welfare and disruption. While the number of devices connected to the Internet continues to increase (in the order of billions), so does the number of connection points and scope of data that hackers can exploit. For this reason, the challenge of securing the Internet of Things is one of urgent and widespread concern.

This module examines IoT through the lens of cyber security. We begin with a deep dive into what IoT is, how it works, and what societal benefits it offers. Attention is then turned to the security vulnerabilities of IoT devices and ecosystems in homes and business settings, and the various ways in which threat actors may exploit IoT data for malicious purposes. This supports learning around how to mitigate risks to IoT security through zero-trust principles and security by design. During the module we take time also to build a critical understanding of the data privacy concerns that surround IoT, as well as recent efforts to establish standards and best practice for IoT security.

18 **Outline syllabus**

- What is IoT and how does it work?
- The societal benefits of IoT
- System architectures and communication technologies/protocols
- The type of scope of data generated by IoT ecosystems
- Data proliferation and privacy concerns

	● Emerging threats and threat actors ● IoT security exploits ● The race for standardisation ● Balancing innovation and risk management ● IoT risk mitigation: retrofitting, zero-trust principles and security by design	
19	**Teaching and learning activities** *Class Hours* Lectures and seminars examine the applications, technologies and benefits of IoT, as well as their security vulnerabilities. You engage some of these vulnerabilities practically in lab sessions, and draw on emerging standards and approaches to securing IoT systems. *Independent Learning* As IoT and IoT security is an evolving topic, it is important that you keep up to date with case studies and developments in the field.	
20	**Intended learning outcomes** *By successful completion of the module, you will be able to demonstrate*	*How assessed*
	1. Systematic knowledge of the application, societal benefits and key architectures of IoT systems.	F2, S1, S2
	2. The ability to consolidate professional perspectives and insights from case study to critically evaluate ethical concerns that surround IoT.	F1, F2, S1
	3. The ability to systematically evaluate the vulnerabilities of IoT systems, and identify how such vulnerabilities may be exploited by threat actors.	F1, S1, S2
	4. The ability to select, critically evaluate and synthesis information for a variety of sources to propose approaches to managing risk in the context of IoT security.	F2, S2
21	**Assessment and feedback** *Formative exercises and tasks:* F1. Group presentation on IoT security threats. F2. Lab exercises and discussions.	
	Summative assessments:	Weighting
	S1. IoT portfolio.	50%
	S2. IoT security solution (2,500 words).	50%

22 **Learning resources**

University Library print, electronic resources and Minerva:

Key texts:

- Russell, B. and Duren, D. (2018) *Practical Internet of Things security: design a security framework for an Internet connected ecosystems.* Packt Publishing.
- Greengard, S. (2015) *The Internet of Things*. MIT Press.
- Gupta, A. (2019) *The IoT hacker's handbook: a practical guide to hacking the Internet of Things.* Apress.
- Mamood, Z. (2021) *Connected vehicles in the Internet of Things: concepts, technologies and frameworks for the IoV.* Springer.
- Wilkins, N. (2019) *Internet of Things: what you need to know about IoT, big data, predictive analytics, artificial intelligence, machine learning, cybersecurity, business intelligence, augmented reality and our future.* Bravex Publications.

Key web-based and electronic resources:

- The WIRED guide to the Internet of Things - www.wired.com/story/wired-guide-internet-of-things
- Ken Munro on Internet of Things Security (Tedx Talk) - search at https://www.youtube.com/
- Cyber risk in an Internet of Things world (Deloitte) - search at https://www2.deloitte.com
- IoT Security Foundation - https://www.iotsecurityfoundation.org
- UK government Secure by Design agenda (2020) - https://www.gov.uk/government/collections/secure-by-design
- NIST publications on IoT - https://www.nist.gov
- China's Internet of Things (US China Economic and Security Review Commission - 2018) - available at https://www.uscc.gov
- LinkedIn Learning videos and course on IoT and IoT security. Accessible via the Bath Spa Library website - https://www.bathspa.ac.uk/library/library-databases

23 **Preparatory work**

For an overview of the territory we cover in this module, read the WIRED guide to the Internet of Things and watch Ken Munro's Tedx Talk on Internet of Things Security.

1	Module code	CYS6003-20			
2	Module title	Cyber Offence			
3	Subject	Cyber Security			
4	Core, Required or Required* for	BSc (Hons) Cyber Security			
5	Level	4	5	**6**	7
6	UK credits	20			
7	ECTS credits	10			
8	Optional for	N/A			
9	Excluded combinations	N/A			
10	Pre-requisite or co-requisite	N/A			
11	Class contact time: total hours	Total Hours: 39			
12	Independent study time: total hours	Total Hours: 161			
13	Semester(s) of delivery	Semester 2			
14	Main campus location	Newton Park			
15	Module co-ordinator	John Curry			
16	Additional costs involved	N/A			
17	**Brief description and aims of module** Internet users, corporate or individual, are under sustained attack by hackers. Whether receiving a random phishing email or a targeted attack by an advanced persistent threat, a successful defence requires understanding the attacker mindset. Some hackers are individuals, others are part of crime syndicates or nation states, but in all cases being able to view targets from their perspective is an invaluable and essential skill for cyber security practitioners. This module puts you in the position of the hacker with an array of tools and techniques that expose and exploit vulnerabilities in target systems. You learn by emulating the ‘red team’ attack process, from digital reconnaissance and intelligence gathering through extracting data and covering your tracks. This form of ethical hacking is a valuable method used by all types of organisations to audit their defences and management processes. By understanding how hackers hack, your defensive awareness and skills are developed, enabling you to identify and mitigate weaknesses in enterprise systems.				
18	**Outline syllabus** ● How ‘threat actors’ identify targets and establish a foothold by compromising servers, endpoints, devices and user accounts. ● The roles of ethical hacking and penetration testing in cyber security, and their rules of engagement ● How to systematically employ open-source security assessment tools to discover vulnerabilities ● Using Red Team offensive tactics to exploit vulnerabilities during simulated attacks ● Techniques of command and control: website shell, outbound web connections, protocol tunnelling, Internet facing accounts ● Techniques of escalating privileges: password capture, session hijacking, exploit vulnerabilities ● Methods of moving laterally: network mapping, remote shell ● Persistence: Methods of maintaining access and avoiding detection ● How hackers steal (confidentiality), modify (integrity) and destroy data				

	(availability)	
19	**Teaching and learning activities** *Class Hours* This module is delivered through a blend of lectures and workshops that include simulation exercises. Practical sessions develop the mindset and explore the actions required to successfully penetrate system defenses. Discursive sessions examine the consequences of cyber crime to individuals, enterprises and nation states, and the ethical considerations of offensive tactics. *Independent Learning* You are expected to follow up concepts introduced in class, regularly review credible sources that describe instances of cyber attack/defence, and conduct simulation exercises as set by the tutor.	
20	**Intended learning outcomes** *By successful completion of the module, you will be able to demonstrate:*	*How assessed*
	1. Comprehensive knowledge of the motivations, objectives, organisation and offensive tactics of the red teaming methodology.	F1, F2, S1
	2. The ability to establish a critical position on the use of offensive tactics that consolidates ethical concerns in the field of cyber security and the practical objectives of organisational cyber resilience.	F2, S1
	3. The ability to apply specialist tools in a systematic manner to identify and critically assess the vulnerabilities of an isolated network.	F1, S1
	4. The ability to critically analyse the findings of cyber offence activities in order to devise insights and recommendations that aim to improve the security posture of a hypothetical organisation.	F1, F2, S1
21	**Assessment and feedback** *Formative exercises and tasks:* F1. Red teaming activities. F2. Discussion and debate forums.	
	Summative assessments:	Weighting
	S1. Cyber offence simulations (5,000 words).	100%

22	**Learning resources** *University Library print, electronic resources and Minerva:* *Key texts:* ● Flow, S. (2017) *How to hack like a GOD: master the secrets of hacking through real life scenarios*. Independently published. ● Kim, P. (2018) *The hacker playbook 3: practical guide to penetration testing.* Independently Published. ● Mitnick, K. and Simon, W. L. (2012) *Ghost in the wires: my adventures as the world's most wanted hacker.* Bay Back. ● Picolet, J. (2020) *Operator handbook: red team + OSINT + blue team reference.* Independently Published. ● Pillay, R. (2019) *Learn penetration testing: understand the art of penetration testing and develop your white hat hacker skills*. Packt Publishing. *Key web-based and electronic resources:* ● Immersive Labs. Access provided for free if signing up using BSU email address - http://immersivelabs.online/ ● National Cyber Security Centre - https://www.ncsc.gov.uk/section/education-skills/higher-education ● MITRE Att&ck Framework - https://attack.mitre.org/ *Specialist resources:* ● NMAP - https://nmap.org ● Open source intelligence gathering tools ● Isolated physical networking devices
23	**Preparatory work** Complete the LinkedIn Learning course on Ethical Hacking and chapter quizzes. Please visit the Bath Spa Library website to access LinkedIn Learning - https://www.bathspa.ac.uk/library/library-databases/

1	Module code	CYS6004-20			
2	Module title	Cyber Defence			
3	Subject	Cyber Security			
4	Core, Required or Required* for	BSc (Hons) Cyber Security			
5	Level	4	5	**6**	7
6	UK credits	20			
7	ECTS credits	10			
8	Optional for	N/A			
9	Excluded combinations	N/A			
10	Pre-requisite or co-requisite	N/A			
11	Class contact time: total hours	Total Hours: 39			
12	Independent study time: total hours	Total Hours: 161			
13	Semester(s) of delivery	Semester 2			
14	Main campus location	Newton Park			
15	Module co-ordinator	John Curry			
16	Additional costs involved	N/A			

17 **Brief description and aims of module**

Our world is dependent on digital technology and this technology is under greater threat from attackers than ever before. Cyber security is critical to defend enterprise systems, as well as personal computing. As attacks evolve, so must the techniques for securing systems. The ongoing challenges facing information security professionals require diligence, readiness and pragmatism. At all times, the effort spent on defence must be proportional to the level of threat and the potential costs associated with compromise.

This module takes you through some of the key technologies, hardware and software that are essential in the layered defences that keep systems operational and the hackers out. You learn by following 'blue team' processes to assess flaws and vulnerabilities, and apply hardening techniques to mitigate risks. The aim is to build a layered system of controls to generate a defence in depth model - a cross between a maze and a digital minefield. Defences are continually monitored and adapted as new threats are discovered and technologies become available.

18 **Outline syllabus**

- Defining the challenge of securing systems
- Risk management - assessing network vulnerabilities
- Business security challenges
- Building an effective defence - defence in depth
- Managing defence through technical and administrative controls
- Responding and managing incidents
- The role and application of threat intelligence

19 **Teaching and learning activities**

Class Hours

Seminar sessions are discursive, with a strong emphasis on individual and group research. Simulation exercise and related practical activities provide an opportunity to evaluate defensive operations in hypothetical settings.

	Independent Learning You are expected to follow up concepts introduced in class, regularly review credible sources that describe instances of cyber attack/defence, and conduct simulation exercises as set by the tutor.	
20	**Intended learning outcomes** *By successful completion of the module, you will be able to demonstrate:*	*How assessed*
	1. Comprehensive knowledge of the motivations, objectives, organisation and defensive tactics of the blue teaming methodology, and the ability to critically evaluate its relationship with red teaming.	F1, F2, S1
	2. The ability to systematically evaluate a hypothetical attack scenario, and propose technical and administrative security controls that are informed by a critical understanding of the concept of defense in depth.	F1, F2, S1
	3. Critical understanding of the scope and function of threat intelligence, and the ability to apply it in a systematic manner in order to improve the security posture of a hypothetical organisation.	F1, F2, S1
	4. The ability to devise, co-ordinate, and adapt in response to new intelligence, a strategy for managing organisational risk in the context of cyber security.	F2, S1
21	**Assessment and feedback** *Formative exercises and tasks:* F1. Blue teaming activities. F2. Discussion and debate forums.	
	Summative assessments:	Weighting
	S1. Risk management strategy (5,000 words).	100%

22 **Learning resources**

University Library print, electronic resources and Minerva:

Key texts:

- Donaldson et al (2018). *Enterprise cybersecurity study guide: how to build a successful cyberdefense program against advanced threats*. Apress.
- Diogenes, Y. and Ozkaya, E. (2018). *Cybersecurity - attack and defense strategies: infrastructure security with red team and blue team tactics*. United Kingdom: Packt Publishing.
- Picolet, J. (2020) *Operator handbook: red team + OSINT + blue team reference.* Independently Published.

	Key web-based and electronic resources: ● LinkedIn Learning has many training courses around the field of pen testing. Accessible via the Bath Spa Library website - https://www.bathspa.ac.uk/library/library-databases ● Action Fraud (UK) https://www.actionfraud.police.uk/ ● National Cyber Crime Unit https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime ● Immersive Labs. Access provided for free if signing up using BSU email address - http://immersivelabs.online/ *Specialist resources:* ● CyberCIEGE - https://nps.edu/web/c3o/cyberciege ● NMAP - https://nmap.org ● Isolated physical networking devices
23	**Preparatory work** Identify a recent incident of cyber attack reported in the media or credible web resource. Take some time to consider how the attack succeeded and which defensive controls proved to be inadequate.

1	Module code	CYS6005-20			
2	Module title	Critical Infrastructure			
3	Subject	Cyber Security			
4	Core, Required or Required* for	BSc (Hons) Cyber Security			
5	Level	4	5	**6**	7
6	UK credits	20			
7	ECTS credits	10			
8	Optional for	N/A			
9	Excluded combinations	N/A			
10	Pre-requisite or co-requisite	N/A			
11	Class contact time: total hours	Total Hours: 52			
12	Independent study time: total hours	Total Hours: 148			
13	Semester(s) of delivery	Semester 2			
14	Main campus location	Newton Park			
15	Module co-ordinator	John Curry			
16	Additional costs involved	N/A			

17 **Brief description and aims of module**

Clustered under the term ‘critical national infrastructure’ (CNI) are organisations, assets and supply chains that manage and deliver national provisions related to health, defence, communications, transport, power, water and emergency services, amongst others. Each of these sectors are exposed to threats from cyber criminals, terrorists and hostile states, with some critical services being more prone than others to espionage, data theft and disruption. CNI cyber resilience is therefore an important concern for the continued functioning of society. Indeed, securing key public and private sector services from cyber attack is an important component of the UK government’s National Security Strategy.

In this module you learn what CNI comprises and why it is vulnerable to cyber attack. Using real world examples, you examine in detail how critical systems are breached and what steps are necessary to withstand such breaches. This includes a critical understanding of approaches to CNI cyber resilience, with particular interest in procedures for threat resistance and strategies for response/recovery. Supporting topics cover the scope and type of threats against CNI, as well as the motivations and objectives of threat actors that target critical infrastructure. Although the UK is a focus in this module, the knowledge and perspectives you encounter can be applied with some adjustment in international contexts.

18 **Outline syllabus**

- What CNI is why it is important
- Critical national infrastructure services in the UK
- The scope and Interconnectivity of CNI
- Threats and hostile actions against CNI
- The motivations and objectives of threat actors
- The implication of successful attacks
- Threat mitigation and discovery
- CNI cyber resilience

19 **Teaching and learning activities**

	Class Hours Lecture and seminar activities expand on the concept of CNI, as well as facilitate discussion on relevant threats and cyber resilience strategies. Practical tasks include, amongst others, critically evaluating potential vulnerabilities to CNI services using data gathered from publicly accessible sources. *Independent Learning* Learning outside of class hours includes examination and analysis of case studies and theoretical scenarios. We recommend also that you keep up to date with publications such as the NCSC weekly threat report, as these occasionally provide insights on CNI security.	
20	**Intended learning outcomes** *By successful completion of the module, you will be able to demonstrate*	*How assessed*
	1. Systematic knowledge of CNI in the context of cyber security, including current threats, the motivations of threat actors and the implications of successful attack.	F1, S1, S2
	2. The ability to identify and apply tools and data sources as needed to conduct a systematic evaluation of the security vulnerabilities of a CNI system.	F1, F2, S1, S2
	3. The ability to critically evaluate and consolidate established strategies for CNI cyber resilience, and devise recommendations for their application in a specific scenario.	F1, F2, S2
	4. The ability to select, critically evaluate, adapt and apply methods of reporting in the cyber security sector in order to communicate the findings of a vulnerability assessment to specialist audiences.	F1, S2
21	**Assessment and feedback** *Formative exercises and tasks:* F1. Case studies analysis of CNI attacks. F2. Investigative activities.	
	Summative assessments:	Weighting
	S1. Presentation. On an example of an attack against critical national infrastructure (10 minutes).	30%
	S2. Vulnerability assessment (3,500 words).	70%
22	**Learning resources** *University Library print, electronic resources and Minerva:* *Key texts:*	

	● Austin, G. (2020) *National cyber emergencies: the return to civil defence*. Routledge. ● Buchanan, B. (2020) *The hacker and the state: cyber attacks and the new normal of geopolitics.* Harvard University Press. ● Johnson T. (2020) *Cybersecurity: protecting critical Infrastructures from cyber attack and cyber warfare.* Routledge. ● Keupp, M. (2020) *The security of critical infrastructures: risk, resilience and defence*. Springer. ● Lewis, T. (2020) *Critical infrastructure protection in homeland security: defending a networked nation*. Wiley. *Key web-based and electronic resources:* ● Centre for Protection of Critical National Infrastructure (CPNI) https://www.cpni.gov.uk ● Cyber Security of UK Infrastructure (2017) - https://post.parliament.uk/research-briefings/post-pn-0554/ ● CPNI YouTube channel https://www.youtube.com/user/UKCPNI ● UK Cabinet Office Public Summary of Sector Security and Resilience Plans (2018) - https://www.gov.uk/government/publications/sector-security-and-resilience-plans-2018-summary ● Reports on critical national infrastructure and cyber security from US Government Accountability Office - https://www.gao.gov/ ● NCSC weekly threat reports - https://www.ncsc.gov.uk/section/keep-up-to-date/threat-reports
23	**Preparatory work** Read the contents of ‘Cyber Security of National Infrastructure’, a POSTnote published by UK Parliament. This provides an overview of the topics we cover in this module.