University of Essex | Online



BSC (HONS) CYBER SECURITY

Course Brochure

ABOUT THE BSC (HONS) CYBER SECURITY

The Details

Indicative duration: 4 years
Qualification: BSc (Hons)

Entry Requirements

Applicants must hold three A-levels or equivalent from an internationally recognised institution. For the work experience entry route, applicants must have GCSE Maths and English at grade C or above, or equivalent, and at least three years' work experience in the IT, computer science or business sector.

Our BSc (Hons) Cyber Security is designed to equip you with a comprehensive understanding of key principles, theories, and practices in Cyber Security. This course is ideal whether you're looking to enter the field of computing or wanting to make a career change.

During the course, you'll gain a global and strategic perspective, enabling you to understand and address the challenges and opportunities presented by globalisation and emerging technologies in Cyber Security.

Upon completion, you'll have gained the relevant knowledge and skills to step into a wide range of roles – including as a Cyber Consultant, Chief Information Security Officer, Security Architect or Forensic Analyst.

You could also choose to study the shorter, 16-month CertHE Cyber Security.

Teaching and Assessment

Teaching methods and style
Unlike a traditional university environment, our online degrees utilise a Virtual Learning Environment (VLE), providing you with immediate access to learning materials, wherever you are.

Student support
You'll be supported throughout your studies by a dedicated Student Adviser and regularly interact with fellow students and your tutor.

Methods of assessment
Instead of exams, we adopt an assignment-based approach to assessment, which are based on real-life work experience and carried out by tutors on an ongoing basis.

SYLLABUS

The BSc (Hons) Cyber Security is made up of the following modules and equal to a total of 360 credits.

Level 4 modules

- Research and Professional Practice (15 credits) ▲§
- Introduction to Maths and Statistics (15 credits) ▲§
- Fundamentals of Programming (15 credits) ▲§
- Object-oriented Programming (15 credits) ▲§
- Fundamentals of Networks (15 credits) ▲§
- Introduction to Cyber Security (15 credits) ▲§
- Ethical Hacking Penetration Testing (15 credits) ▲§
- Operating Systems Security (15 credits) ▲§

Level 5 modules

- Research and Professional Practice 2 (15 credits) ▲
- Software Engineering Fundamentals (15 credits)
- Computer Security (15 credits) ▲
- Introduction to AI (15 credits)
- Digital Forensics (15 credits) ▲
- Cryptography (15 credits) ▲
- Data Visualisation and Communication (15 credits) ▲
- Behavioural Cyber Security (15 credits) ▲

Level 6 modules

- Capstone Project (45 credits) ▲
- Information Retrieval (15 credits)
- Network Security (15 credits)
- Data Ethics and Leadership (15 credits)
- Information Security and Risk Management (15 credits)
- Security Operations and Incident Response (15 credits)

▲ Core module (must be passed in order to achieve the award)
§ Modules included in CertHE Cyber Security

LEVEL 4
MODULES

RESEARCH AND PROFESSIONAL PRACTICE

Module code: RAPP_UCOM4E	**NQF level:** 4
Credit value: 15	**Study duration:** 9 weeks

About the module

Develop the foundational knowledge of computing as this module introduces discussions, practical exercises, and real-world case studies, to help you develop essential skills including critical thinking, effective communication and data analysis. You'll also learn about sustainability principles and how your research can contribute to sustainable development goals.

Learning outcomes

On completion of this module, you'll be able to:

- demonstrate an understanding of the research process, including formulating research questions, conducting literature reviews, and designing research methodologies
- apply ethical principles and considerations in the planning, execution, and reporting of research activities
- utilise appropriate data collection methods and analytical techniques to address research questions and objectives
- communicate research findings effectively through written reports and oral presentations
- reflect on their professional development and identify opportunities for future growth and specialization in research and professional practice

Syllabus

- Introduction to research and professional practice
- Literature review and critical analysis
- Research design and methodology
- Data collection methods & data analysis techniques
- Research ethics
- Writing and presenting research findings
- Professional development and future directions

Learning and teaching methods

Teaching will be delivered through a series of units covering the topics specified in the syllabus with a focus on developing computing knowledge and skills. Students are directed in their learning to specified reading materials on the virtual learning platform and online peer discussion is encouraged.

Regular interactive online seminar sessions are scheduled with the module tutor covering a variety of complementary topics and practical skills related to the course aims and objectives. Tutor support is available to students via phone, email, Zoom/ Skype and synchronous seminar sessions, as required.

Description of unit assessment	Duration	Submission date	Weighting
Individual research proposal	1,000 words	End of Unit 6	20%
Individual mini research project	3,000 words	End of Unit 9	80%

INTRODUCTION TO MATHS AND STATISTICS

Module code: IMS_UCOM4E	**NQF level:** 4
Credit value: 15	**Study duration:** 9 weeks

About the module

In this module, you'll learn the basic mathematics and statistics that are required in the computer science field. Topics that will be covered include the use of counting methods, the application of basic notions of sets, summary statistics and hypothesis testing.

Learning outcomes

On completion of this module, you'll be able to:

- apply proposition logic and counting methods including permutations and combinations to simple problems
- utilise the basic notions of sets and illustrate answers using Venn diagrams
- solve problems in linear algebra using vectors and matrices
- employ summary statistics to solve problems
- interpret statistical findings using probability and hypothesis

Syllabus

- Propositional logic
- Combinatorics
- Sets
- Vectors and matrices
- Descriptives statistics
- Probability
- Hypothesis testing and statistical significance
- Parametric tests
- Nonparametric tests

Learning and teaching methods

This module will be delivered via specified learning materials on the VLE and supported by lecturecasts, readings and weekly seminars, where peer discussion is encouraged. Tutors will also be available via phone, email and video call.

Description of unit assessment	Duration	Submission date	Weighting
Quiz	1 hour	End of Unit 2	30%
Collaborative discussion	300 words	End of Unit 4	20%
Test	1.5 hours	End of Unit 9	50%

FUNDAMENTALS OF PROGRAMMING

Module code: FOP_UCOM4E	**NQF level:** 4
Credit value: 15	**Study duration:** 9 weeks

About the module

This module aims to provide foundational programming skills by covering the basics and EDI principles. You'll develop entrepreneurial thinking to drive the creation of inclusive and sustainable software. During your studies, you'll utilise Python to write, test, and debug while gaining essential skills such as critical problem-solving abilities.

Learning outcomes

On completion of this module, you'll be able to:

- understand basic programming concepts and constructs, such as variables, data types, control structures, functions, and arrays
- design algorithms to solve simple problems
- implement algorithms using a high-level programming language (e.g. Python)
- analyse code to debug and test appropriately

Syllabus

- Introduction to procedural programming
- Abstraction in programming
- A model of memory
- Basics of the programming language
- Statements and control flow
- Functions in depth
- Data structures: lists and dictionaries
- Input and output
- Integration and practical applications

Learning and teaching methods

This module will be delivered by specified learning materials on the VLE and supported by lecturecasts, readings and weekly seminars, where peer discussion is encouraged. Tutors will also be available via phone, email and video call.

Description of unit assessment	Duration	Submission date	Weighting
Individual coursework	700 words	End of Unit 4	10%
Collaborative discussion	300 words	End of Unit 4	20%
End of module: Individual coursework	3,000 words (equivalence)	End of Unit 9	70%

OBJECT-ORIENTED PROGRAMMING

Module code: OOP_UCOM4E	**NQF level:** 4
Credit value: 15	**Study duration:** 9 weeks

About the module

Gain an understanding of object-oriented programming principles (OOP) and methodologies as this module introduces you to essential OOP concepts and techniques such as inheritance, polymorphism, encapsulation, abstraction and design patterns. You'll also be encouraged to consider sustainability principles throughout your studies.

Learning outcomes

On completion of this module, you'll be able to:

- demonstrate a thorough understanding of object-oriented programming principles and concepts
- understand existing software systems to identify opportunities for refactoring and improvement using object-oriented methodologies
- design and implement object-oriented software solutions using appropriate design patterns and programming techniques
- apply object-oriented design principles to model real-world problems and develop basic software applications using object-oriented programming techniques

Syllabus

- Introduction to object-oriented programming
- Classes and objects
- Inheritance and polymorphism
- Encapsulation and abstraction
- Exception handling
- Design patterns
- Software development practices
- Practical application and projects
- Testing and debugging

Learning and teaching methods

This module will be delivered by specified learning materials on the VLE and supported by lecturecasts, readings and weekly seminars, where peer discussion is encouraged. Tutors will also be available via phone, email and video call.

Description of unit assessment	Duration	Submission date	Weighting
Individual coursework	2,000 words	End of Unit 4	30%
Practical test	Two hours (2,000 words equivalent)	End of Unit 9	70%

FUNDAMENTALS OF NETWORKS

Module code: FON_UCOM4E	**NQF level:** 4
Credit value: 15	**Study duration:** 9 weeks

About the module

Gain a comprehensive understanding of computer networking as you progress through this module. You'll explore thought-provoking topics such as network architecture, protocols, models, services and security considerations, and take part in different workshop and practical sessions to practise your skills.

Learning outcomes

On completion of this module, you'll be able to:

- explain a network architecture to examine the network protocols, models, services, potential issues, and security considerations in implementing specific networking requirements
- modify and configure the network devices by applying the necessary settings
- design IP sub-networks with a particular focus on learning subnetting principles and addressing schemes
- evaluate, propose, and justify the implementation of suitable protocols for networked applications, and explain the principles governing Ethernet and IP networking

Syllabus

- Introduction to networking concepts
- Definition, types, and classifications of computer networks, Network Models and Protocols
- Network protocols and communications
- Network access including the introduction to network access control, authentication and authorization mechanisms, and network access policies and security considerations
- Basics of ethernet including the frame structure and ethernet switch configurations and VLANs
- Network layer and routing
- IP Addressing
- Subnetting IP networks
- Transport Layer Protocols
- Introduction to application layer protocols (HTTP, FTP) and configurations
- Design considerations for small networks including hardware and software requirements

Learning and teaching methods

This module will be delivered via specified learning materials on the VLE and supported by lecturecasts, readings and weekly seminars, where peer discussion is encouraged. Tutors will also be available via phone, email and video call.

Description of unit assessment	Duration	Submission date	Weighting
Coursework	2,000 words	End of Unit 4	50%
Practical test	Two hours (2,000 words equivalent)	End of Unit 9	50%

INTRODUCTION TO CYBER SECURITY

Module code: ICS_UCOM4E	**NQF level:** 4
Credit value: 15	**Study duration:** 9 weeks

About the module

Learn about the concepts of threats and vulnerability within cyber security. You'll review the principle of non-repudiation and be introduced to examples of mitigations including encryption, digital signatures and hardware devices such as firewalls and intrusion prevention systems. By the end of your studies, you'll develop entrepreneurship knowledge and skills in relevant contexts.

Learning outcomes

On completion of this module, you'll be able to:

- articulate the strategies for addressing problems in applications that deal with security and privacy.
- gain proficiency in employing techniques for tasks such as vulnerability assessments, threat modelling and security management.
- apply security principles to IT applications and infrastructure.
- explain the use of critical methods for evaluating cyber security risks and mitigations.
- understand the application of cybersecurity principles to application and system design.

Syllabus

- What is cyber security and why does it matter?
- The basics of security theory
- Security concepts, standards and assurance
- Common threats and vulnerabilities
- Threat modelling
- Cyber defence and mitigations
- Enterprise implications of cyber security

Learning and teaching methods

This module will be delivered via specified learning materials on the VLE and supported by lecturecasts, readings and weekly seminars, where peer discussion is encouraged. Tutors will also be available via phone, email and video call.

Description of unit assessment	Duration	Submission date	Weighting
Coursework	2,000 words	End of Unit 4	50%
Exam	2,000 words	End of Unit 9	50%

ETHICAL HACKING PENETRATION TESTING

Module code: EHPT_UCOM4E	**NQF level:** 4
Credit value: 15	**Study duration:** 9 weeks

About the module

This module explores the principles and practices of ethical hacking and penetration testing. You'll focus on various topics including identifying vulnerabilities, testing system security and understanding the ethical implications of hacking. You'll also gain hands-on experience with tools and techniques, while developing a deep understanding of cybersecurity frameworks and policies.

Learning outcomes

On completion of this module, you'll be able to:

- explain the legal and ethical boundaries of penetration testing.
- perform reconnaissance and scanning to gather information on targets.
- conduct vulnerability assessments and exploit security weaknesses.
- demonstrate the use of industry-standard tools for penetration testing.
- prepare professional penetration testing reports with recommendations for mitigation.

Syllabus

- Introduction to ethical hacking and legal frameworks
- Reconnaissance and information gathering
- Scanning and enumeration
- Vulnerability assessment
- Exploitation
- Post-exploitation techniques
- Penetration methods
- Reporting and mitigation
- Emerging trends and advanced topics

Learning and teaching methods

This module will be delivered via specified learning materials on the VLE and supported by lecturecasts, readings and weekly seminars, where peer discussion is encouraged. Tutors will also be available via phone, email and video call.

Description of unit assessment	Duration	Submission date	Weighting
Collaborative case study analysis	1,000 words	Unit 4	30%
Practical test	2 hours (1,500 words equivalent)	Unit 9	70%

OPERATING SYSTEMS SECURITY

Module code: OSS_UCOM4E	**NQF level:** 4
Credit value: 15	**Study duration:** 9 weeks

About the module

Gain a comprehensive understanding of operating system (OS) security. During this module, you'll explore critical security mechanisms, learn to secure system services and implement best practices for protecting sensitive data. The module also emphasises the principles of Equality, Diversity and Inclusion (EDI) to foster an understanding of how inclusive practices can strengthen OS security management.

Learning outcomes

On completion of this module, you'll be able to:

- develop a comprehensive understanding of security mechanisms.
- design and apply authentication protocols and manage access control models.
- apply OS hardening and secure configuration techniques.
- enhance security in Linux Environments.
- develop effective system monitoring and patch management strategies.

Syllabus

- OS security foundations
- User authentication and access control
- Secure configuration and hardening
- Linux security
- Memory and kernel-level security
- File system security
- Event logging and system auditing
- OS updates and patch management

Learning and teaching methods

This module will be delivered by specified learning materials on the VLE and supported by lecturecasts, readings and weekly seminars, where peer discussion is encouraged. Tutors will also be available via phone, email and video call.

Description of unit assessment	Duration	Submission date	Weighting
Practical assignment	2,000 words	End of Unit 4	50%
Case study report	2,000 words	End of Unit 9	50%

LEVEL 5
MODULES

RESEARCH AND PROFESSIONAL PRACTICE 2

Module code: RAPP_UCOM5E	**NQF level:** 5
Credit value: 15	**Study duration:** 9 weeks

About the module

In this module, you'll be involved in projects that are based around research, allowing you to enhance your teamwork and professional skills. This is by diving into various aspects including effective project and time management strategies, design principles, legal implications, health and safety protocols.

Learning outcomes

On completion of this module, you'll be able to:

- apply design methodology effectively to formulate a design that aligns with specified requirements
- execute a project utilising adept time management skills and producing comprehensive progress reports
- employ a systematic approach to gather, analyse, and present data at a professional standard
- investigate and furnish reports on the sustainability parameters related to projects or products, displaying an understanding of environmental impact and considerations, including ethical and legal aspects

Syllabus

- Introduction to comprehensive skill development
- Teamwork dynamics and methodologies
- Data gathering, analysis, and reporting
- Project management and product development
- Professional issues and individual contributions

Learning and teaching methods

The module will be taught via the VLE and supported by reading materials, online discussions, tutor-led forums and regular team meetings. You'll also display your abilities through an e-portfolio to reflect on your personal growth and CPD. Weekly drop-in sessions are available with your module tutor for support and clarification on topics.

Description of unit assessment	Duration	Submission date	Weighting
Group project report	1,500 words	End of Unit 4	25%
Research Proposal	2,500 words	End of Unit 9	75%

SOFTWARE ENGINEERING FUNDAMENTALS

Module code: SEF_UCOM5E	**NQF level:** 5
Credit value: 15	**Study duration:** 9 weeks

About the module

Investigate the fundamental concepts and practices of software engineering with a focus on sustainability, while this module emphasises teamwork, communication, and engagement. During your studies, you'll discover various topics including the design, implementation, testing, deployment, and maintenance of software development lifecycles.

Learning outcomes

On completion of this module, you'll be able to:

- understand then apply the principles of software engineering to manage software projects
- design software applications using modern development methodologies
- evaluate appropriate software design patterns and architectures
- understand ethical considerations in software development and how to address them

Syllabus

- Introduction to software engineering and SDLC
- Software requirements and design principles
- Software development methodologies
- Version control and software design patterns
- Software testing
- Agile methodologies and project management
- Software quality assurance and maintenance
- Ethical and professional issues
- Integration, deployment, and continuous delivery

Learning and teaching methods

This module will be delivered via specified learning materials on the VLE and supported by lecturecasts, readings and weekly seminars, where peer discussion is encouraged. Tutors will also be available via phone, email and video call.

Description of unit assessment	Duration	Submission date	Weighting
Group coursework assignment	10-minute presentation 1,000 words	End of Unit 4	20%
Implementation assignment	3,000 words total equivalent	End of Unit 9	80%

COMPUTER SECURITY

Module code: CS_UCOM5E	**NQF level:** 5
Credit value: 15	**Study duration:** 9 weeks

About the module

This module introduces the general principles of cybersecurity from a theoretical and practical perspective. You'll explore the fundamental concepts such as cryptography, access policy models, user authentication protocols and operating system security. You'll also move on to advanced topics such as malware analysis and computer forensics.

Learning outcomes

On completion of this module, you'll be able to:

- define and explain core concepts and terminologies related to cyber security.
- describe common security vulnerabilities.
- explain the nature of malware and how it can spread, identified and removed.
- compare cryptography systems and their implementation.
- identify and explain the principle of risk analysis and how to implement risk management in computer security.

Syllabus

- Introduction to cybersecurity
- Principles of cryptography
- Application of encryption to computer security
- Authentication and access control
- Operating system security
- Threat modelling: malware analysis
- Computer security in practice

Learning and teaching methods

This module will be delivered via specified learning materials on the VLE and supported by lecturecasts, readings and weekly seminars, where peer discussion is encouraged. Tutors will also be available via phone, email and video call.

Description of unit assessment	Duration	Submission date	Weighting
Case study report	1,500 words	End of Unit 4	50%
E-portfolio and reflective piece	2,500 words total	End of Unit 9	50%

INTRODUCTION TO ARTIFICIAL INTELLIGENCE

Module code: IAI_UCOM5E	**NQF level:** 5
Credit value: 15	**Study duration:** 9 weeks

About the module

Delve into the three pivotal assets of artificial intelligence in this insightful module. Explore the methodologies and techniques of search algorithms, knowledge representation and learning mechanisms and discover how they hold central significance in related fields, such as computer games and robotics.

Learning outcomes

On completion of this module, you'll be able to:

- critically evaluate arguments both in favour of and against the feasibility of artificial intelligence.
- explain and implement standard blind and heuristic search procedures.
- demonstrate an understanding of strengths, weaknesses and practical applications for solving well-defined problems.
- show comprehension of the functionality of standard production system interpreters.
- articulate the workings of various established machine learning procedures.
- understand agent-oriented approach to artificial intelligence.
- explain the construction of a multi-agent system consisting of purely reactive agents using a subsumption architecture

Syllabus

- Introduction to AI
- Problem-solving through searching
- Using knowledge to solve problems
- Acquiring knowledge through machine learning
- Intelligent agents

Learning and teaching methods

This module will be delivered via specified learning materials on the VLE and supported by lecturecasts, readings and weekly seminars, where peer discussion is encouraged. Tutors will also be available via phone, email and video call.

Description of unit assessment	Duration	Submission date	Weighting
AI proficiency portfolio	1,500 words	End of Unit 4	40%
AI application mini project	2,500 words	End of Unit 9	60%

DIGITAL FORENSICS

Module code: DF_UCOM5E	**NQF level:** 5
Credit value: 15	**Study duration:** 9 weeks

About the module

Explore the fundamental principles and methodologies used in digital forensics in this module. You'll discover a range of topics such as forensic investigation processes, tools and techniques for retrieving, preserving and analysing digital evidence. By the end, you'll have gained useful skills including analytical skills for investigating digital crimes and cyber incidents.

Learning outcomes

On completion of this module, you'll be able to:

- explain the key principles, processes and methodologies of digital forensics.
- analyse and interpret digital evidence from various sources.
- demonstrate proficiency in using forensic tools for data recovery and analysis.
- apply legal, ethical and professional standards in forensic investigations.
- conduct a forensic investigation, document findings and prepare reports.

Syllabus

- Introduction to digital forensics
- Legal and ethical considerations
- Forensic process and methodology
- File system forensics
- Network and cloud forensics
- Memory and mobile forensics
- Malware analysis and incident response
- Forensic tools and techniques
- Case studies and practical exercises

Learning and teaching methods

This module will be delivered via specified learning materials on the VLE and supported by lecturecasts, readings and weekly seminars, where peer discussion is encouraged. Tutors will also be available via phone, email and video call.

Description of unit assessment	Duration	Submission date	Weighting
Individual collaborative discussion	1,000 words	End of Unit 4	20%
Case study and report	3,000 words	End of Unit 9	80%

CRYPTOGRAPHY

Module code: C_UCOM5E	**NQF level:** 5
Credit value: 15	**Study duration:** 9 weeks

About the module

In this module, you'll investigate a comprehensive range of cryptographic methods – encryption, decryption, hashing, digital signatures and key management. By the end, you'll possess the analytical and technical proficiency needed to design, implement and evaluate secure cryptographic solutions.

Learning outcomes

On completion of this module, you'll be able to:

- explain the fundamental concepts, principles and techniques underpinning classical and modern cryptography.
- analyse and evaluate different cryptographic algorithms and their applications.
- implement cryptographic algorithms using programming languages and tools to secure data and communication.
- assess security challenges and propose cryptographic solutions for specific scenarios.

Syllabus

- Introduction to cryptography
- Classical cryptographic techniques
- Symmetric key cryptography
- Asymmetric key cryptography
- Cryptographic hash functions
- Digital signatures and certificates
- Key management and cryptographic protocols
- Security attacks and countermeasures
- Emerging trends in cryptography

Learning and teaching methods

This module will be delivered via specified learning materials on the VLE and supported by lecturecasts, readings and weekly seminars, where peer discussion is encouraged. Tutors will also be available via phone, email and video call.

Description of unit assessment	Duration	Submission date	Weighting
Individual report	1,500 words	Unit 4	30%
Practical implementation and presentation	1,500 words	Unit 9	70%

DATA VISUALISATION AND COMMUNICATION

Module code: DVC_UCOM5E	**NQF level:** 5
Credit value: 15	**Study duration:** 9 weeks

About the module

Gain the skills to transform complex data into clear, effective and visually compelling representations in this module. Discover the key principles of design, perception and storytelling, and explores various visualisation techniques, from basic charts to interactive and dynamic graphics. You'll also gain hands-on experience using industry-standard tools and libraries to create meaningful visualisations.

Learning outcomes

On completion of this module, you'll be able to:

- critically analyse and assess the effectiveness of different visualisation methods based on principles of design, perception and usability.
- demonstrate the ability to design and implement effective data visualisations using appropriate tools and techniques to represent complex datasets clearly and accurately.
- use industry-standard data visualisation libraries and software to create interactive and dynamic visual representations of data.
- effectively communicate data-driven insights through visual storytelling, written reports and presentations tailored to different audiences.

Syllabus

- Introduction to data visualisation
- Principles of effective visualisation
- Data preparation and cleaning for visualisation
- Advanced visualisation techniques
- Visual storytelling and communication
- Ethical considerations and bias in data visualisation

Learning and teaching methods

This module will be delivered via specified learning materials on the VLE and supported by lecturecasts, readings and weekly seminars, where peer discussion is encouraged. Tutors will also be available via phone, email and video call.

Description of unit assessment	Duration	Submission date	Weighting
Individual coursework	2,500 words	Unit 4	40%
Presentation	10 minutes / 1.500 words	Unit 9	60%

BEHAVIOURAL CYBER SECURITY

Module code: BCS_UCOM5E	**NQF level:** 5
Credit value: 15	**Study duration:** 9 weeks

About the module

This module covers the intersection of human behaviour, psychology and cybersecurity – exploring intriguing topics including cognitive biases, social engineering and organisational culture. You'll also examine how human factors contribute to security vulnerabilities and designing effective, ethical strategies that promote secure behaviours in both organisational and individual contexts.

Learning outcomes

On completion of this module, you'll be able to:

- demonstrate a comprehensive understanding of the role human behaviour plays in cybersecurity.
- apply relevant psychological and behavioural theories to analyse and mitigate cybersecurity risks in organisational and individual contexts.
- develop and evaluate strategies to influence user behaviour and improve adherence to cybersecurity best practices.
- critically evaluate the ethical and societal implications of behaviour-focused cybersecurity interventions.

Syllabus

- Cyber threat and the threat environment
- Human factors and cybersecurity implications
- Psychology of cybersecurity
- Behaviour change models
- Dimensions of security culture
- Security culture framework
- Professionalism

Learning and teaching methods

This module will be delivered via specified learning materials on the VLE and supported by lecturecasts, readings and weekly seminars, where peer discussion is encouraged. Tutors will also be available via phone, email and video call.

Description of unit assessment	Duration	Submission date	Weighting
Analysis report	2,000 words	Unit 4	50%
Presentation	10 minutes / 2,000 word equivalent	Unit 9	50%

LEVEL 6
MODULES

CAPSTONE PROJECT

Module code: CP_UCOM6E	**NQF level:** 6
Credit value: 45	**Study duration:** 27 weeks

About the module

In this module, you'll demonstrate the practical skills and academic knowledge you've gained throughout your studies. You'll have the opportunity to show off your creativity, innovation, and academic and professional abilities by carrying out a significant piece of independent research or extensive practical project on a topic within computer science.

Learning outcomes

On completion of this module, you'll be able to:

- synthesise and integrate knowledge and skills from various disciplines to define and approach a complex problem.
- apply appropriate research methodologies, tools and techniques to conduct in-depth investigation.
- critically analyse and evaluate findings to draw evidence-based conclusions.
- demonstrate creativity and innovation in proposing solutions or recommendations for the project focus area.
- exhibit professional skills including project management, ethical considerations and effective communication.
- reflect on the learning process and the application of skills in a professional context.

Syllabus

- Introduction and project proposal
- In-depth research and development
- Mid-project review and analysis
- Finalising project
- Completion and presentation

Learning and teaching methods

This module will be delivered via specified learning materials on the VLE and supported by lecturecasts, readings and weekly seminars, where peer discussion is encouraged. Tutors will also be available via phone, email and video call.

Description of unit assessment	Duration	Submission date	Weighting
Research proposal	1,500 words	Unit 5	10%
Poster	1,500 words	Unit 16	10%
Final report	6,000 words	Unit 25	60%
Presentation	10 slides / 1,000 words	Unit 26	10%
Planning and reflective log	2,000 words	Unit 27	10%

INFORMATION RETRIEVAL

Module code: IR_UCOM6E	**NQF level:** 6
Credit value: 15	**Study duration:** 9 weeks

About the module

In this module, you'll learn how to design energy-efficient information retrieval systems. You'll delve into the theoretical foundations of information retrieval (IR) systems including text processing, indexing and querying, while considering the carbon footprint of digital information processing. By the end, you'll understand how to build environmentally friendly IR systems that drive social and economic value.

Learning outcomes

On completion of this module, you'll be able to:

- understand the core principles and models of information retrieval.
- design and implement efficient text processing, indexing and querying systems.
- apply ranking algorithms and relevance feedback mechanisms to improve search results.
- evaluate the performance of IR systems using standards metrics.

Syllabus

- Introduction to Information Retrieval
- Text processing and normalisation
- Indexing and search techniques
- Ranking algorithms and relevance
- Evaluation of IR systems
- Web crawling and search engines
- Machine learning for information retrieval
- Advanced topics in IR
- Case studies

Learning and teaching methods

This module will be delivered via specified learning materials on the VLE and supported by lecturecasts, readings and weekly seminars, where peer discussion is encouraged. Tutors will also be available via phone, email and video call.

Description of unit assessment	Duration	Submission date	Weighting
Individual coursework	10-minutes / 1,000 words equivalent	End of Unit 4	40%
Research report	3,000 words	End of Unit 9	60%

NETWORK SECURITY

Module code: NS_UCOM6E	**NQF level:** 6
Credit value: 15	**Study duration:** 9 weeks

About the module

This module explores the principles, techniques and tools used to secure computer networks. You'll also cover topics such as network analysis, threat assessment and cryptographic approaches, and how these apply to real-life scenarios. By the end, you'll understand how to keep computer networks safe from cyber-attacks.

Learning outcomes

On completion of this module, you'll be able to:

- demonstrate understanding of the fundamentals of network security and its importance in modern computing environment.
- identify and describe common network security vulnerabilities/attacks.
- design computer network architecture that reduces security risk.
- describe and implement cryptographic techniques for encryption and authentication.
- display an understanding of the operation of security tools for network security applications.
- demonstrate knowledge of IPS/IDS and formulate appropriate firewall table rules for secure networks.

Syllabus

- Introduction to network security
- Network architecture and protocols
- Cryptographic techniques for network security
- Access control and authentication
- Network threats and vulnerabilities
- Implementing secure communication protocols
- Designing a secure network
- Virtual Private Networks (VPNs)
- Network security best practices and case studies

Learning and teaching methods

This module will be delivered via specified learning materials on the VLE and supported by lecturecasts, readings and weekly seminars, where peer discussion is encouraged. Tutors will also be available via phone, email and video call.

Description of unit assessment	Duration	Submission date	Weighting
Case study report	2,000 words	End of Unit 4	50%
Object recognition mini project	2,000 words	End of Unit 9	50%

DATA ETHICS AND LEADERSHIP

Module code: DEL_UCOM6E	**NQF level:** 6
Credit value: 15	**Study duration:** 9 weeks

About the module

Explore the ethical considerations and leadership challenges in managing and leveraging data within the cyber security domain. By the end of this module, you'll be able to handle sensitive data, address ethical dilemmas and developing policies that ensure data security and compliance.

Learning outcomes

On completion of this module, you'll be able to:

- articulate key ethical frameworks and their relevance to data management in cyber security.
- analyse the impact of regulatory policies on cyber security practices.
- evaluate case studies involving ethical dilemmas in data use and propose solutions.
- demonstrate leadership skills in formulating and implementing data ethics policies.

Syllabus

- Introduction to data ethics and leadership
- Regulatory frameworks and compliance
- Privacy, security and ethical dilemmas
- Leadership strategies in ethical decision-making
- Corporate responsibility and risk assessment

Learning and teaching methods

This module will be delivered via specified learning materials on the VLE and supported by lecturecasts, readings and weekly seminars, where peer discussion is encouraged. Tutors will also be available via phone, email and video call.

Description of unit assessment	Duration	Submission date	Weighting
Ethical analysis report	1,500 words	End of Unit 4	40%
Leadership strategy plan	2,500 words	End of Unit 9	60%

INFORMATION SECURITY AND RISK MANAGEMENT

Module code: ISRM_UCOM6E	**NQF level:** 6
Credit value: 15	**Study duration:** 9 weeks

About the module

This module will introduce you to the concepts of information security, data classification, and breach analysis and management. You'll have the opportunity to handle each stage of the risk management process in detail, supplemented by case studies and examples as appropriate, and consider the principles of equality, diversity and inclusivity (EDI).

Learning outcomes

On completion of this module, you'll be able to:

- articulate the strategies for addressing problems in Information Security classification and Management.
- gain proficiency in employing techniques for tasks such as risk assessments, risk modelling and information security management.
- apply information security and risk principles to IT applications and infrastructure.
- understand the use of critical methods to evaluate information security risks and determine mitigations.
- display an understanding of the application of the risk management process to information security solutions.

Syllabus

- What is information security risk management and why does it matter?
- The basics of the risk management process
- Risk concepts, tools and classification
- Risk identification and assessment
- Risk modelling, analysis and frameworks
- Incident response planning
- Enterprise implications of information security management

Learning and teaching methods

This module will be delivered via specified learning materials on the VLE and supported by lecturecasts, readings and weekly seminars, where peer discussion is encouraged. Tutors will also be available via phone, email and video call.

Description of unit assessment	Duration	Submission date	Weighting
Coursework	2,000 words	End of Unit 5	50%
Presentation	2,000 words equivalent	End of Unit 9	50%

SECURITY OPERATIONS AND INCIDENT RESPONSE

Module code: SOIR_UCOM6E	**NQF level:** 6
Credit value: 15	**Study duration:** 9 weeks

About the module

Gain a comprehensive understanding of the principles and practices essential for managing cybersecurity incidents. You'll explore key topics including assessing security posture, understanding the cybersecurity kill chain, and identifying and mitigating attack vectors – such as reconnaissance and privilege escalation.

Learning outcomes

On completion of this module, you'll be able to:

- analyse advanced concepts in security posture and incident response to design and implement robust security operations in complex organisational security.
- examine the cybersecurity kill chain, reconnaissance techniques and privilege escalation to evaluate threats and develop strategies to disrupt attack paths effectively.
- demonstrate expertise in investigating security incidents by collecting, analysing and interpreting digital evidence, including log files and forensic data, to produce comprehensive investigative reports.
- design and apply innovative threat-hunting methodologies and implement advanced vulnerability management practices to safeguard systems against sophisticated cyberattacks.
- formulate and execute advanced recovery strategies, including system hardening and post-incident reviews.

Syllabus

- Advanced cybersecurity frameworks and operations
- Cyber threat landscape
- Incident investigation
- Proactive security measures
- Post-incident activities

Learning and teaching methods

This module will be delivered via specified learning materials on the VLE and supported by lecturecasts, readings and weekly seminars, where peer discussion is encouraged. Tutors will also be available via phone, email and video call.

Description of unit assessment	Duration	Submission date	Weighting
Report	2,000 words	End of Unit 5	50%
Report and reflective piece	2,000 words total	End of Unit 9	20%

READY TO APPLY?

online.essex.ac.uk

+44 (0) 1206 489 358 | enquiries@online.essex.ac.uk