Prifysgol Wrecsam
Wrexham University

Module specification

When printed this becomes an uncontrolled document. Please access the Module Directory for the most up to date version by clicking on the following link: Module directory

Module Code	COM668
Module Title	Cyber Security
Level	6
Credit value	20
Faculty	FACE
HECoS Code	100376
Cost Code	GACP
Pre-requisite module	None

Programmes in which module to be offered

Programme title	Core/Optional/Standalone
BSc (Hons) Computing for Business	Core

Breakdown of module hours

Learning and teaching hours	12 hrs
Placement tutor support hours	0 hrs
Supervised learning hours e.g. practical classes, workshops	12 hrs
Project supervision hours	0 hrs
Active learning and teaching hours total	**24 hrs**
Placement hours	0 hrs
Guided independent study hours	176 hrs
Module duration (Total hours)	**200 hrs**

Module aims

The aim of this module is to develop students' knowledge and critical understanding of the principles, practices, and challenges of cyber security in modern business contexts. It will enable students to evaluate threats, vulnerabilities, and risks to information systems, and to apply appropriate tools, techniques, and policies to protect organisational assets. The module emphasises both the technical aspects of securing networks, systems, and data, and the wider business, ethical, and legal considerations of cyber security. Students will also be encouraged to critically assess emerging security technologies and strategies, preparing them to contribute effectively to the protection of digital systems within professional environments.

Module Learning Outcomes

At the end of this module, students will be able to:

1	Critically evaluate the core principles, key concepts, and terminology of cyber security, including the nature of threats, vulnerabilities, and risk management strategies.
2	Apply appropriate tools, techniques, and frameworks to secure systems, networks, and data in business environments.
3	Analyse and evaluate security risks and incidents in organisational contexts, identifying weaknesses and proposing suitable mitigation strategies.
4	Design, evaluate, and justify security solutions that address technical, organisational, and human factors, demonstrating awareness of current and emerging trends and threats in cyber security.

Assessment

Indicative Assessment Tasks:
This section outlines the type of assessment task the student will be expected to complete as part of the module. More details will be made available in the relevant academic year module handbook.

The assessment for this module will be coursework-based and designed to measure both the technical and critical dimensions of cyber security. Students will complete a range of tasks that demonstrate their ability to apply tools and techniques, analyse risks, and evaluate security practices within business contexts. Assessments will be structured to allow students to demonstrate progression from understanding core principles to designing and justifying robust security solutions.

Typical assessment activities may include practical security exercises, case study analysis, incident response scenarios, reflective reports, and written assignments. These activities will enable students to showcase their technical competence in applying security tools, as well as their ability to evaluate organisational, legal, and ethical considerations.
Portfolio assessments may comprise multiple pieces of work that collectively demonstrate a student's knowledge and skills developed throughout the module. These may take the form of one or two substantial tasks, or a series of smaller tasks, typically ranging from one to eight across the duration of the module.

Assessment number	Learning Outcomes to be met	Type of assessment	Duration/Word Count	Weighting (%)	Alternative assessment, if applicable
1	1, 2, 3.,4	Portfolio	4000 Words or Equivalent	100%	N/A

Derogations

N/A

Learning and Teaching Strategies

In line with the Active Learning Framework, this module will be blended digitally with both a VLE and online community. Content will be available for students to access synchronously and asynchronously and may indicatively include first and third-party tutorials and videos, supporting files, online activities any additional content that supports their learning. As this module progresses, the strategies will change to best support a diverse learning environment. For each week, a topic will be started with tutor-led demonstrations, and practical-based sessions will be given to ensure that the students get to practice what they have been taught in relevant concepts. Sessions will be intertwined between instructional explanation and practical depending on the specific indicated syllabus necessities.

Welsh Elements

This module is designed to support Welsh-speaking students in line with the Welsh Language Standards. While the primary delivery will be in English, students will have the opportunity to submit assessments, including coursework and projects, in Welsh if preferred. Relevant module materials, such as reading lists, key texts, and guidance, will be available bilingually upon request, ensuring accessibility for all students. Additionally, where possible, guest speakers, case studies, or examples may include references to the Welsh business context, especially in areas such as data use in local industries and Welsh public sector organisations.

The department encourages students to develop bilingual digital skills by incorporating Welsh-language datasets, tools, and resources where appropriate, offering an inclusive learning environment. We also support the development of bilingual visualisation techniques, enabling students to create digital outputs that reflect the Welsh language, should they wish to do so.

Indicative Syllabus Outline

- Foundations: Cyber security principles, threats, vulnerabilities, risk frameworks
- Network and System Security: Authentication, access control, encryption, firewalls, intrusion detection
- Risk and Incident Management: Risk assessment, monitoring, auditing, incident response, digital forensics
- Human and Organisational Factors: Social engineering, insider threats, building a security culture
- Legal and Ethical Issues: UK and international legislation, compliance, professional responsibilities
- Evaluation and Testing: Penetration testing, vulnerability assessment, security audits
- Emerging Trends: Cloud and IoT security, mobile threats, AI in cyber defence, evolving attack surfaces

Indicative Bibliography

Please note the essential reads and other indicative reading are subject to annual review and update.

Essential Reads:

There are no essential texts; the module will use relevant online reference material.

Other indicative reading:

- Stallings, W. and Brown, L. (2024), *Computer Security: Principles and Practice*. 5th ed. Harlow: Pearson.
- Pfleeger, C.P. (2024), *Security in Computing*. 6th ed. Boston: Pearson Education.
- Whitman, M.E. & Mattord, H.J., 2022. Principles of Information Security. 7th ed. Cengage Learning.
- Anderson, R., 2020. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Wiley.
- NIST (National Institute of Standards and Technology), 2018. Framework for Improving Critical Infrastructure Cybersecurity. [online] Available at: https://www.nist.gov/cyberframework [Accessed 30 August 2025].
- European Union Agency for Cybersecurity (ENISA), 2023. Threat Landscape Report. [online] Available at: https://www.enisa.europa.eu/publications [Accessed 30 August 2025].

Administrative Information

For office use only	
Initial approval date	29th January 2026
With effect from date	September 2026
Date and details of revision	
Version number	1