Module Specification

Cyber Security Project

Version: 2026-27, v3.0, Approved

Contents

Part 1: Information

Module title: Cyber Security Project

Module code: UFCE8A-30-3

Level: Level 6

For implementation from: 2026-27

UWE credit rating: 30

ECTS credit rating: 15

College: College of Arts, Technology and Environment

School: CATE School of Computing and Creative Technologies

Partner institutions: None

Field: Computer Science and Creative Technologies

Module type: Module

Pre-requisites: None

Excluded combinations: None

Co-requisites: None

Continuing professional development: No

Professional, statutory or regulatory body requirements: None

Part 2: Description

Overview: The cyber security project is an individual research project which enables the student to select and investigate a topic of interest within Cyber Security beyond the normal level of treatment in the taught modules. It is primarily self-directed study and is required to align with a Cyber Security Body of Knowledge (CyBOK) domain of the students choice.

Features: Not applicable

Educational aims: The cyber security project is an individual research project which enables the student to select and investigate a topic of interest within Cyber Security beyond the normal level of treatment in the taught modules. It is primarily an academic intellectual exploration of a relevant CyBOK related topic through software development, primary research or secondary research. A key component of the module is exposure to the rigors of researching, planning and time management associated with any significant individual study and through this exposure to provide a focus for the development of appropriate tools, skills and disciplines necessary for the successful completion of the project.

Outline syllabus: The subject of the project may stem from the student's own interests, perhaps developed from their placement or other prior experience, or from the research interests of staff. The only constraint is that the project must align with the CyBOK.

In all cases students are expected to: identify clear aims and scope for their investigation; undertake a survey of relevant literature; treat material critically and demonstrate their understanding of the relationship between material covered in the taught modules and the specific topic studied. The literature survey may be supplemented with empirical work or software development if the student wishes. In concluding the project, students should appraise their achievements in relation to the stated aims of their investigation and the methods used to research and write up the project.

Part 3: Teaching and learning methods

Teaching and learning methods: Scheduled learning includes start of year briefings and workshops followed by regular supervision meetings, as described above.

Independent learning hours includes: engaging with literature searching and reading; analysis, synthesis and critical review of relevant material; drafting and refining dissertation content. Independent work may also involve attendance at workshops

and talks relevant to the student's chosen topic, as well as engagement with online resources and subject experts, as appropriate to the topic.

Students are required to submit a poster and an accompanying video recording as a milestone assessment. Furthermore, opportunities will be provided for students to present their ongoing progress to staff and peers.

Module Learning outcomes: On successful completion of this module students will achieve the following learning outcomes.

MO1 Professionally investigate and critically appraise a chosen topic aligned with the Cyber Security Body of knowledge (CyBOK).

MO2 Present and articulate project findings succinctly and professionally.

MO3 Plan, manage, complete and review a significant piece of independent written work.

MO4 Demonstrate timely progress and engagement with a self-directed research project.

Hours to be allocated: 300

Contact hours:

Independent study/self-guided study = 282.5 hours

Staff-guided learning = 17.5 hours

Reading list: The reading list for this module can be accessed at readinglists.uwe.ac.uk via the following link https://rl.talis.com/3/uwe/lists/E3276F72-FE64-E207-6D2E-6FC934D267B0.html?lang=en&login=1

Part 4: Assessment

Assessment strategy: Assessment is based on three tasks: a milestone submission part-way through the module and, at the end of the module, a written report and an oral viva/demonstration. The milestone submission consists of a poster and video detailing progress so far, and is assessed on a Pass/Fail basis. The written report documents the project in full, including the investigation of the problem,

the approach taken, the work undertaken, the evaluation of outcomes, and critical reflection on the project as a whole. The viva/demonstration will assess the student's understanding, critical engagement, and ability to articulate and defend the decisions and outcomes of the project work.

Detailed assessment criteria will be published annually in the module handbook but will include the following:
Alignment with the CyBOK (mandatory);
Clarity of definition of aims and scope of the project;
Breadth and/or depth, currency, and appropriateness of academic content;
Use of appropriate perspectives and techniques to evaluate evidence and construct arguments;
Structure, clarity, and accuracy of written and oral expression;
Effectiveness of project planning and self-management;
Accuracy and consistency in citation and referencing using UWE Harvard format.

Formative assessment is provided primarily through regular supervision sessions, where students receive tailored feedback on their progress, project scope, literature review, and overall methodological approach. This ongoing formative feedback helps students refine their ideas, improve their academic skills, and ensures alignment with module requirements and CyBOK domains ahead of the summative assessments.

It is expected that the resit will normally involve the student revising and improving their original submission based on feedback. A new project submission may be permitted but is generally discouraged. Resit candidates for the poster and video will reflect the final project outcomes instead of ongoing progress.

Assessment tasks:

Poster (First Sit)
Description: Project Progress Poster with supporting video
Weighting: 0 %
Final assessment: No
Group work: No

Learning outcomes tested: MO4

Report (First Sit)
Description: Report (6000 - 8000 words)
Weighting: 30 %
Final assessment: No
Group work: No
Learning outcomes tested: MO1, MO3

Presentation (First Sit)
Description: Viva/Demonstration (45 Mins)
Weighting: 70 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO2

Poster (Resit)
Description: Project Progress Poster with supporting video
Weighting: 0 %
Final assessment: No
Group work: No
Learning outcomes tested: MO4

Report (Resit)
Description: Report (6000 - 8000 words)
Weighting: 30 %
Final assessment: No
Group work: No
Learning outcomes tested: MO1, MO3

Presentation (Resit)
Description: Viva/Demonstration (45 Mins)
Weighting: 70 %
Final assessment: Yes

Group work: No

Learning outcomes tested: MO2

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Cyber Security and Digital Forensics [Frenchay] BSc (Hons) 2023-24

Cyber Security and Digital Forensics [Frenchay] BSc (Hons) 2024-25

Cyber Security and Digital Forensics [NepalBrit] BSc (Hons) 2024-25

Cyber Security and Digital Forensics {Foundation} [Frenchay] BSc (Hons) 2023-24

Cyber Security and Digital Forensics {Foundation} [Frenchay] BSc (Hons) 2022-23