Module Specification

Cyber Security Project

Version: 2024-25, v2.0, 11 Jan 2024

Contents

Part 1: Information

Module title: Cyber Security Project

Module code: UFCE8A-30-3

Level: Level 6

For implementation from: 2024-25

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 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. Termly larger group review meetings will also be scheduled to help students take stock of their progress, receive feedback from staff and peers and adjust their plans to ensure successful completion of the module.

Independent learning includes hours: 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.

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 Communicate succinctly their finding.

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

Hours to be allocated: 300

Contact hours:

Independent study/self-guided study = 282.5 hours

Face-to-face learning = 17.5 hours

Total = 300

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 the final written report, including supporting evidence and information included as appendices. The report should be a maximum of 8,000 words in length, excluding appendices. 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 dissertation;

breadth and/or depth, currency and appropriateness of academic content underpinning;

use of appropriate perspectives and techniques to marshal and evaluate arguments and evidence from a range of sources;

structure, layout, clarity and accuracy of expression and overall argument;

accuracy, completeness and consistency of citation and listing of sources, in UWE Harvard format .

evidence of effective project planning and management, self-evaluation and learning.

The student may choose to submit an entirely new project at resit, but will generally be discouraged from doing so. It is expected that normally the resit will involve the student reworking their original submission to remedy the deficiencies identified in the feedback.

Assessment tasks:

Project (First Sit)
Description: A report of not less than 6,000 and not more than 8000 words.
Weighting: 100 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1, MO2, MO3

Project (Resit)
Description: A report of not less than 6,000 and not more than 8000 words.
Weighting: 100 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1, MO2, MO3

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Cyber Security and Digital Forensics [NepalBrit] BSc (Hons) 2022-23

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

Cyber Security and Digital Forensics {Foundation} [Sep][FT][Frenchay][4yrs] BSc (Hons) 2021-22