Module Specification

Cyber Security Futures Emerging Trends and Challenges

Version: 2023-24, v2.0, 13 Mar 2023

Contents

Part 1: Information

Module title: Cyber Security Futures Emerging Trends and Challenges

Module code: UFCFXN-15-M

Level: Level 7

For implementation from: 2023-24

UWE credit rating: 15

ECTS credit rating: 7.5

Faculty: Faculty of Environment & Technology

Department: FET Dept of Computer Sci & Creative Tech

Partner institutions: None

Delivery locations: Frenchay Campus

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: Developments in cyber security are impacted by many different influences, for example, technological advance, changes in law, social change and attitude to technology. Any of these areas and others may be of interest in this module.

Features: Not applicable

Educational aims: The module is delivered as a series of workshops and will provide students with an opportunity to engage in supported horizon scanning in order to identify and explore emerging trends in cyber security.

Outline syllabus: See educational aims and teaching and learning methods.

Part 3: Teaching and learning methods

Teaching and learning methods: At start of the module, students are guided to discuss the characteristics of cyber security. These discussions might include the notion that cyber security is a rapidly evolving discipline and is influenced by subtle and unpredictable changes in human behaviour, economic change, development of new hardware etc.

Based on these initial discussions and under the tutor's guidance, students will then begin to explore relevant research areas and domains of interest. Such topics should be aligned with existing relevant knowledge frameworks, e.g. CyBOK.

The chosen topics are then explored on a week by week basis by a combination of individual student research, (possibly) invited speakers and student presentations.

These sessions are supplemented by workshops that explore key aspects of conducting an investigation such as the identification of aims and objectives; conducting a literature review and the use of critique.

The outcomes from these workshop discussions will form a collective body of knowledge in cyber security trends.

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

MO1 Evaluate and critique the current trends and challenges in cyber security

MO2 Report on evidenced speculation about likely future trends and their impact

MO3 Communicate complex information clearly and effectively

Hours to be allocated: 150

Contact hours:

Independent study/self-guided study = 114 hours

Face-to-face learning = 36 hours

Total = 150

Reading list: The reading list for this module can be accessed at readinglists.uwe.ac.uk via the following link https://uwe.rl.talis.com/index.html

Part 4: Assessment

Assessment strategy: This assignment requires the students to write a proposal for funding competition based on a real call. However, the intention of this work is to evaluate the skills and knowledge students acquired in this module by analysing emerging cybersecurity research trends and challenges during the seminar activities.

The assignment is based on individual work (report) (100%) where the focus is to produce a research-driven contribution in the emerging areas of cybersecurity. Students need to evaluate their solution and create a product prototype or a solution design that has commercial value.

In the referral assessment, students can improve their previous submission or choose a new topic to complete the assessment requirements. It will be the same as the main assessment, 100% report.

Assessment components:

Report (First Sit)
Description: Report. Max word limit: 2000
Weighting: 100 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1, MO2, MO3

Report (Resit)

Description: Report. Max word limit: 2000

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 [Frenchay] MSc 2023-24

Cyber Security [GCET] MSc 2023-24

Cyber Security [Frenchay] MSc 2022-23