MODULE SPECIFICATION

Part 1: Information			
Module Title	Cyber Threats		
Module Code	UFCFFU-30-1	Level	Level 4
For implementation from	2020-21		
UWE Credit Rating	30	ECTS Credit Rating	15
Faculty	Faculty of Environment & Technology	Field	
Department	FET Dept of Computer Sci & Creative Tech		
Module type:			
Pre-requisites	None		
Excluded Combinations	None		
Co- requisites	None		
Module Entry requirements	None		

Part 2: Description

Overview:
Security is one of the most important challenges modern organisations face. Security is about protecting organisational assets, including personnel, data, equipment and networks from attack through the use of prevention techniques in the form of vulnerability testing/security policies and detection techniques, exposing breaches in security and implementing effective responses.

In order to provide protection, it is fundamental to understand the types of threats, their methods and means of attack.

In this module you will explore the different types of threat.

Educational Aims: Contributes to foundation knowledge. Explores cyber threats in the context of the concepts explored in other L4 modules.

Outline Syllabus: You will cover:

foundations of cyber security, its significance, concepts, threats, vulnerabilities and assurance

application of cyber security concepts to IT infrastructure

fundamental building blocks and typical architectures of IT infrastructure

common vulnerabilities in networks and systems

vulnerabilities in computer networks, applications and systems (e.g., insecure coding and unprotected networks) and how they can be exploited

network-based attacks e.g.:
eavesdropping/sniffing, man-in-the-middle, spoofing, session hijacking, denial of service, traffic redirection, routing attacks, traffic analysis

impact of vulnerabilities in an organisational context

human dimension of cyber security and adversarial thinking applied to system development

how an employee may enable a successful attack chain without realising it

factors that may increase or decrease risks related to an organisation's 'cyber culture'

links between physical, logical, personal and procedural security

ways to defend against cyber attack

adversarial thinking in the context of system development, application development and analysis

the threat landscape, threat trends, horizon scanning

the threat intelligence lifecycle and the concepts of threat actors and attribution

the significance, value and limitations of threat analyses

Teaching and Learning Methods:
Lecture sessions cover the technical knowledge required. Designated practical work is included to give the students the opportunity to explore the technical knowledge in a hands-on fashion and the ensure that they have absorbed and understood the key principles involved.

Part 3: Assessment

This module is assessed by a combination of: a threat analysis presentation (30 minutes) and a research report (3000 words)

Component A
Students will carry out a threat analysis for their employer's IT systems or a subset of them. The methods, results and recommendations will be presented.

Component B
Students will consolidate their knowledge and begin to practice their research skills by researching current cyber threats and ranking them in order of probability. This will also ensure that the module remains current and engaging for the students. Examples should be given for each type of threat, the specific vulnerability they attacked and what could have mitigated the impact.

At referral, students will rework any deficiencies from the main sit, using feedback to guide them.

First Sit Components	**Final Assessment**	**Element weighting**	**Description**

Presentation - Component A	✓	50 %	Presentation on a threat analysis.
Project - Component B		50 %	Report on current cyber threats.
Resit Components	**Final Assessment**	**Element weighting**	**Description**
Presentation - Component A	✓	50 %	Re-worked presentation
Report - Component B		50 %	Re-worked report.

Part 4: Teaching and Learning Methods

Learning Outcomes

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

Module Learning Outcomes	**Reference**
Discover, identify and analyse typical threats, attack techniques, vulnerabilities and mitigations.	MO1
Research and explain the incidence of various types of threat over time and their methods to attack common vulnerabilities.	MO2
Explain how to mitigate against cyber-attacks employing a range of appropriate methods.	MO3
Carry out a threat analysis .	MO4

Contact Hours

Independent Study Hours:	
Independent study/self-guided study	135
Total Independent Study Hours:	135
Placement Study Hours:	
Placement	75
Total Placement Study Hours:	75
Scheduled Learning and Teaching Hours:	
Face-to-face learning	90
Total Scheduled Learning and Teaching Hours:	90

	Hours to be allocated	300
	Allocated Hours	300
Reading List	*The reading list for this module can be accessed via the following link:* https://rl.talis.com/3/uwe/lists/E44BA897-7E1C-423D-35D0-4514105FAA1E.html	

Part 5: Contributes Towards
This module contributes towards the following programmes of study: BSc (Hons) Cyber Security Technical Professional (integrated degree) BSc (Hons) 2020-21