MODULE SPECIFICATION

When printed this becomes an uncontrolled document. Please access the Module Directory for the most up to date version by clicking here.

Refer to guidance notes for completion of each section of the specification.

Module Code:	CONL719

Module Title:	Cyber Security for Digital Business

Level:	7	**Credit Value:**	15

Cost Centre(s):	GACP	JACS3 **code**: HECoS code:	I190 100366

Faculty	FAST	**Module Leader:**	Jessica Muirhead

Scheduled learning and teaching hours	15 hrs
Placement tutor support	0 hrs
Supervised learning eg practical classes, workshops	0 hrs
Project supervision (level 6 projects and dissertation modules only)	0 hrs
Total contact hours	15 hrs
Placement / work based learning	0 hrs
Guided independent study	135 hrs
Module duration (total hours)	150 hrs

Programme(s) in which to be offered (not including exit awards)	Core	Option
MBA with Cyber Security	✓	☐

Pre-requisites
None

Office use only
Initial approval: 04/06/2020 Version no: 1
With effect from: 01/09/2020
Date and details of revision: 05/05/21 Revision to Essential Text Version no:2

Module Aims
This module will introduce students to the technical and socio-technical aspects of cyber security that challenge businesses in the current environment. Students will explore a number of specific threats, identifying, applying and critically evaluating techniques to secure digital business technologies. All topics follow an applied approach, with material built upon case studies and industry best practices.

Module Learning Outcomes - at the end of this module, students will be able to	
1	Identify, analyse and evaluate a range of cyber security vulnerabilities within an organisational context.
2	Select and explain appropriate procedures, solutions and countermeasures to defend and minimise security attacks.
3	Make informed judgements on organisational cyber security risks.
4	Identify and evaluate weaknesses in business computer systems.
5	Critically evaluate the response of organisations to simulated cyber security incidents.

Employability Skills **The Wrexham Glyndŵr Graduate**	**I = included in module content** **A = included in module assessment** **N/A = not applicable**
Guidance: complete the matrix to indicate which of the following are included in the module content and/or assessment in alignment with the matrix provided in the programme specification.	
CORE ATTRIBUTES	
Engaged	I A
Creative	A
Enterprising	I
Ethical	I A
KEY ATTITUDES	
Commitment	N/A
Curiosity	I A
Resilient	I A
Confidence	I A
Adaptability	I A
PRACTICAL SKILLSETS	
Digital fluency	I A
Organisation	I A
Leadership and team working	I A
Critical thinking	I A

Emotional intelligence	A
Communication	I A

Derogations

None

Assessment:

Indicative Assessment Tasks:

Students will complete a range of portfolio tasks documenting their understanding of the key topics throughout the module (1,500 words equivalent). There will be formative and summative submissions during Weeks 3 and 5 respectively.

This will be followed by a case study report (1,500 words), where students analyse a contemporaneous organisational security incident, preparing an incident response plan and evaluating the effectiveness of the business when responding to threats and vulnerabilities. The report will be due for submission at the end of Week 8.

Assessment number	Learning Outcomes to be met	Type of assessment	Weighting (%)
1	1,2,3	Portfolio	50%
2	4,5	Report	50%

Learning and Teaching Strategies:

The overall learning and teaching strategy is one of guided independent study, in the form of distance learning requiring ongoing student engagement. On-line learning materials will be provided as weekly sessions whereby the student is required to log-in and engage on a regular basis throughout the module. There will be a mix of video recordings, with supporting notes/slides, containing embedded digital content and self-checks for students to complete as they work through the module and undertake their assessed tasks. The use of a range digital tools via the virtual learning environment together with additional sources of reading will also be utilised to accommodate accessibility. The basis for working with online materials will be through self-directed study and regular online communication with tutors/peers. Students are encouraged to interact with each other and tutors through a range of communication tools.

Syllabus outline:

Viruses, malware and ransomware
Authentication
Network and device security; backups
Phishing, social engineering and socio-technical approaches
Web system vulnerabilities
Ethical hacking
Online digital forensics

Indicative Bibliography:
Essential reading
Randell J.Boyle. (2015) Corporate Computer Security, 4th Edition. Pearson.
Other indicative reading
Easttom, C. (2017) *System Forensics, Investigation, and Response.* 3rd ed. Jones and Bartlett Publishers Harper, A. (2018) *Gray Hat Hacking: The Ethical Hacker's Handbook.* 4th ed. New York: McGraw-Hill Education. Howard, M., LeBlanc, D. and Viega, J. (2009), *24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them.* New York: McGraw-Hill Kim, P. (2015) *The Hacker Playbook 2: Practical Guide to Penetration Testing.* CreateSpace.