Title	Cybercrime and Digital Forensics
Long Title	Cybercrime and Digital Forensics
Credits	5
NFQ Level	Expert

Module Description:

Cybercrime includes traditional offences such as fraud and identify theft, to content offences relating to the online distribution of abuse material or acts of terrorism, to offences related to computers and information systems i.e. malware, hacking etc. As part of this module, students will learn about the different categories of cybercrime and legal frameworks and data privacy laws that are used to protect citizens against cybercrime. As part of this module learners will be introduced to the topic of digital forensics and key laws and legislation related to the e-discovery process.

Learning Outcomes

On successful completion of this module the learner will be able to:

LO1	Discuss key trends and drivers in cyber enabled and cyber dependent crime.
LO2	Assess the legal frameworks and tools used to combat traditional cybercrime offences and hybrid threats.
LO3	Evaluate the laws and regulations that are used to prevent and protect women and children against cybercrime.
LO4	Categorise data collected as part of a digital forensics investigation and identify key measures to uncover digital evidence.
LO5	Evaluate the key laws and legislations used as part of an eDiscovery process.

Indicative Content

Cybercrime

What is cybercrime. Different types of cybercrimes. Cost of cybercrime to business and citizens in Ireland and the EU. Trends and key drivers in cybercrime. Advancements in digitalisation and impact of cybercrime. Cyber enabled and cyber dependent crime.

Cybercrime laws and regulations

Irish court cases and court ruling relating to cybercrime. The legislative challenges in combating cybercrime. European Communities (Electronic Communications Networks and Services). Data Protection Directive (95/46/EC) and General Data Protection Regulation (GDPR). E-Privacy regulations. Network and Information Systems (NISD). Payment Service Directive II (PSD2). Defamation Act. The NIS Directive – The first EU cybersecurity law and NIS Directive II.

Hybrid threats and cybercrime

Cybercrime and hybrid threats. Terror, Hacktivism and cyber terror. Nation state attacks. Electronic attacks and cybercrime. EU response in defending cyber space. Cyber Diplomacy Toolbox. Cyber Deterrence Posture. Boosting Cyber Defence capabilities – Cyber Defence Policy Framework (CDPF).

Cybercrime against women and children

Budapest Convention on Cybercrime. Criminal Justice (Offences Relating to Information Systems) Act 2017. Lanzarote Convention. The Criminal Justice (Sexual Offences) Act 2017. Harassment, Harmful Communications and Related Offences Act 2020 (Coco's Law). Irelands position and progress towards fulfilment of the Budapest and Lanzarote conventions.

Digital Forensics and Computer Based Electronic Evidence

Introduction to digital forensics. Uncovering digital evidence. Digital forensics categories. Digital forensics users. Digital forensics investigation types. e-Discovery process in Ireland. Discovery, seizure of computer equipment. Evidence Recovery process. Handling of mobile phones etc. Law enforcement investigation of cybercrime. Rules on cross border access to electronic devices for criminal investigations i.e. e-evidence. Legal challenges in digital forensic investigations.

Course Work

Assessment Type	*Assessment Description*	*Outcome Addressed*	*% of Total*	*Assessment Date*
Project	An example project would be the learner would be presented with a case study and would be expected to critically assess cybercrime and legal frameworks and data privacy laws that are used to protect citizens against cybercrime.	1,2,3	50.0	Week 6
Project	This project will assess the learners knowledge in digital forensics and the laws and regulations surrounding the collection and recovery of digital data.	4,5	50.0	Sem End

No End of Module Formal Exam

Assessment Breakdown	**%**
Coursework	100

Re-Assessment Requirement

Coursework Only

This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.

Workload – Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lectures covering the theoretical concepts underpinning the learning outcomes.	2.00	Every Week	2.00
Lab	Lab to support the learning outcomes.	1.00	Every Week	1.00
Independent & Directed Learning (Non-contact)	Independent learning by the student.	4.00	Every Week	4.00
		Total Hours		7.00
		Total Weekly Learner Workload		7.00
		Total Weekly Contact Hours		3.00

Workload – Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lectures covering the theoretical concepts underpinning the learning outcomes.	2.00	Every Week	2.00
Lab	Lab to support the learning outcomes.	1.00	Every Week	1.00
Independent & Directed Learning (Non-contact)	Independent learning by the student.	4.00	Every Week	4.00
		Total Hours		7.00
		Total Weekly Learner Workload		7.00
		Total Weekly Contact Hours		3.00

Recommended Book Resources

- **Thomas J. Holt, Adam M. Bossler 2017, Cybercrime and Digital Forensics: An Introduction, Routledge [ISBN: 1138238732]**