

WM3A6-15 Cyber Security & Incident Response

27/28

Department

WMG

Level

Undergraduate Level 3

Module leader

Olga Angelopoulou

Credit value

15

Module duration

30 weeks

Assessment

100% coursework

Study location

University of Warwick main campus, Coventry

Description

Introductory description

This module comprises two related but distinct themes: cyber incident response and digital forensics. The focus of the module is on investigations that respond to incidents in corporate environments, while it sets the scene on examining potential evidence based on the principles that have been established by the digital forensics community.

The cyber incident response theme concentrates on enabling an organisation to support its critical services in the face of a cyber incident. The incident response lifecycle is covered from preparation, through monitoring, detection, containment, eradication, restoration and post incident review.

The digital forensics part of the module concentrates on preserving and forensically analysing potential evidence as part of the incident response process. It sets the requirements for digital forensics within the incident response process and explores the techniques that should be followed by a digital forensics investigator.

Module aims

This module aims to provide the students with the required skills that will allow them to prepare and manage a cyber security incident and allow them to apply digital forensics principles for the investigation of a cyber security incident.

Outline syllabus

This is an indicative module outline only to give an indication of the sort of topics that may be covered. Actual sessions held may differ.

The content of this module will be taught from a cyber security perspective.

Planning for cyber incidents

- Incident detection
- Intrusion response: Intrusion management
- Incident handling: Intrusion analysis, monitoring and logging

Digital Forensics

- Collecting, processing and preserving digital evidence
- Host forensics
- Memory forensics
- Network collection and analysis
- Remediation and Reporting

This is an indicative module outline and actual sessions held may differ.

Learning outcomes

By the end of the module, students should be able to:

- Critically evaluate the operation of a cyber incident response plan.
- Develop an incident response plan for a given context
- Investigate digital artefacts against a realistic brief, preserving, analysing, interpreting and reporting significant material.
- Critically evaluate the significant characteristics of relevant tools and techniques.

Indicative reading list

[Reading lists can be found in Talis](#)

[Specific reading list for the module](#)

Interdisciplinary

There is some interdisciplinary element relevant to the nature of the digital forensics part of the module. It involves relevant law elements.

Subject specific skills

Incident response lifecycle and practices, investigation principles, evaluation of a cyber security incident, host based analysis, network based analysis

Transferable skills

Critical thinking, problem solving, communication, technical literacy

Study

Study time

Type	Required
Supervised practical classes	18 sessions of 2 hours (24%)
Private study	54 hours (36%)
Assessment	60 hours (40%)
Total	150 hours

Private study description

Independent activity between workshops, following up on activities initiated in previous workshops or preparing for upcoming workshops.

Costs

No further costs have been identified for this module.

Assessment

You must pass all assessment components to pass the module.

Assessment group A

	Weighting	Study time	Eligible for self-certification
Assessment component			
Proposal of a cyber incident	40%	30 hours	Yes (extension)

	Weighting	Study time	Eligible for self-certification
plan			
Proposal of a cyber incident plan based on a case study.			

Reassessment component

Proposal of a cyber incident plan			No
Proposal of a cyber incident plan based on a case study.			

Assessment component

Investigation of a cyber incident 60%	30 hours	Yes (extension)
Apply investigation techniques on a given cyber incident scenario and produce a technical report that responds to relevant findings.		

Reassessment component

Investigation of a cyber incident		No
Apply investigation techniques on a given cyber incident scenario and produce a technical report that responds to relevant findings.		

Feedback on assessment

Written feedback for each assignment
 Verbal feedback during tutorial sessions
 Solutions provided to selected tutorial questions
 Summative feedback on assignments

Availability

Courses

This module is Core for:

- UWMA-H651 Undergraduate Cyber Security
 - Year 3 of H651 Cyber Security
 - Year 3 of H651 Cyber Security
 - Year 3 of H651 Cyber Security