

WM284-15 Research and Professional Skills

27/28

Department

WMG

Level

Undergraduate Level 2

Module leader

Elzbieta Titis

Credit value

15

Module duration

10 weeks

Assessment

100% coursework

Study location

University of Warwick main campus, Coventry

Description

Introductory description

This module is designed to familiarise students with researching cross-cutting issues in cyber security contexts, introduce them to a range of data collection methods and analytical options relevant to this, and help them develop relevant skills in data collection and analysis. Students will also be introduced to ethical issues in cyber security research, as well as provided with guidance on how to design, plan and manage their dissertation effectively. Lastly, the module will present students with careers-oriented tasks, giving them the opportunity to consider their professional skills and career aspirations.

Module aims

The module aims to equip students with the knowledge and general research tools to correctly execute a project in cyber security. The focus is on the design of a research project, as well as providing students with the professional and teamwork skills to support the course and their overall career in cyber security.

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.

1. Research Methods:

- Evaluating literature.
- Quantitative research method.
- Qualitative research methods.
- Experimental and computational research methods.

1. Professional Skills:

- Regulatory requirements.
- Team roles and personal responsibility.
- Ethics.
- Project management.
- Communication methods.
- Careers guidance.
- Approaches to continuing professional development.
- Construction of a personal development plan.

Learning outcomes

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

- Critically evaluate current and emerging cyber security research or technologies using appropriate criteria and techniques. [CITP 2.1.5., 2.1.9., 3.2.2]
- Select and justify suitable research and project management methods to address a defined cyber security problem, considering ethical implications. [CITP 2.1.3., 2.1.4., 2.1.5., 4.2.2.]
- Communicate complex cyber security concepts effectively to both technical and non-technical audiences, reflecting on the effectiveness of the communication. [CITP 2.3.2]
- Demonstrate commitment to professional development through the creation and justification of a personal development plan. [CITP 2.3.2]

Indicative reading list

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

[Specific reading list for the module](#)

Research element

Discerning appropriate methods for researching cyber security topics.
Negotiating, designing and planing a research project.

Interdisciplinary

Drawing on a range of disciplines relevant to socio-technological domain of cyber security, such as

psychology, sociology, criminology, etc.

Subject specific skills

Discerning appropriate methods for researching cyber security topics.
Negotiating, designing and planing a research project.

Transferable skills

Problem-solving, communication, ethical values, self-management, professionalism.

Study

Study time

Type	Required
Lectures	10 sessions of 1 hour (7%)
Supervised practical classes	20 sessions of 1 hour (13%)
Online learning (independent)	10 sessions of 1 hour (7%)
Private study	50 hours (33%)
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 A1

	Weighting	Study time	Eligible for self-certification
Assessment component			
Essay with integrated PDP	70%	42 hours	Yes (extension)
Students will write a critical essay on a topic related to cyber security research methods and ethics, and integrate therein a Personal Development Plan (PDP) that reflects on their academic and professional growth in this area.			
Reassessment component is the same			
Assessment component			
Research proposal presentation	30%	18 hours	No
In groups, students will devise an investigation into cyber security topic of their choosing. This will be provided in the form of research proposal. Students will present their proposals in class.			
Reassessment component			
Devising research investigation			Yes (extension)
When taken as a resit, this assessment becomes an individual submission (written report).			

Feedback on assessment

Formative feedback during tutorial sessions.
Summative feedback on assignments.

Availability

Courses

This module is Core for:

- UWMA-H651 Undergraduate Cyber Security
 - Year 2 of H651 Cyber Security
 - Year 2 of H651 Cyber Security
 - Year 2 of H651 Cyber Security