# WM186-15 Cyber Security Fundamentals

## 25/26

**Department**
WMG
**Level**
Undergraduate Level 1
**Module leader**
Harjinder Lallie
**Credit value**
15
**Module duration**
30 weeks
**Assessment**
Multiple
**Study location**
University of Warwick main campus, Coventry

---

## Description

## Introductory description

Understanding the steps and common attack patterns associated with cyber is essential to detecting, identifying, mitigating and responding to cyber-attacks.

Working on this module you will develop knowledge of these core concepts. You will also gain insight into how adversaries move from initially probing and performing reconnaissance of targets, to implementing a way to persist and maintain access to a device/network once compromised.

Several frameworks and attack modelling techniques exist to help better understand and conceptualize how adversaries move through the stages of a cyber-attack have come to the forefront of the cyber security industry. These include: attack graphs, attack trees, fault trees, MITRE ATT&CK, Cyber Kill Chain. Some of these techniques enable practitioners to model a cyber-attack using visual methods.

This module equips students to better understand the stages and concepts of a cyber-attack. Additionally, the module will equip and allow students to develop a practical understanding, as well as applying a range of tools, techniques and procedures utilized by adversaries and attackers during each phase of a cyber-attack in a manner that is both legal and ethical.

## Module aims

The module aims to enable students to:

- understand and apply common cyber-attack modelling methods.
- apply the common tools, techniques and procedures associated with cyber-attacks, legally, ethically, and methodically.

## 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 Cyber Security Landscape. The CIA and AAA of cyber security

Attack modelling

- Common cyber-attack modelling systems including: attack graphs, attack trees, fault trees, MITRE ATT&CK, Cyber Kill Chain

Understanding cyber threats, vulnerabilities, and malware

Understanding risks and risk management

Understanding the importance of security awareness and other strategies for dealing with the insider threat.

Cyber crime, adversaries, and adversarial behaviour.

Legal and Ethical considerations

## Learning outcomes

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

- Identify tools, techniques and procedures which are associated with common attacks within the context of cyber-space, using a given framework,
- Compare and contrast the effectiveness of the relevant tools, techniques and procedures of a given cyber-attack framework when employed against a given target system.
- Demonstrate the application of the tools, techniques and procedures of a given cyber-attack framework which may be used by cyber adversaries against a simulated target system.
- Demonstrate the ability to communicate complex cyber-attack primitives to lay audiences concisely, clearly, and professionally

## Subject specific skills

- Select and apply appropriate tools, techniques and procedures related to specific parts of the Cyber Kill Chain.

- Identify tools, techniques and procedures that could be used to mitigate and remediate the actions of an adversary.
- Respond appropriately to situations that challenge legal, ethical and reputational values.

## Transferable skills

Problem solving, critical thinking, creativity, analytical and ethical reasoning

---

## Study

## Study time

| Type | Required |
|---|---|
| Lectures | 18 sessions of 1 hour (12%) |
| Tutorials | 18 sessions of 1 hour (12%) |
| Private study | 54 hours (36%) |
| Assessment | 60 hours (40%) |
| Total | 150 hours |

## Private study description

Private study to strengthen concepts learned in the module

## 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 |
|---|---|---|---|
| Coursework 1 | 35% | 30 hours | Yes (extension) |

May involve the analysis, evaluation, and modelling of a recent cyber-attack represented within a report aimed at given stakeholders

Alternatively, may involve the proposal of strategies aimed at reducing the likelihood of a cyber attack

| | Weighting | Study time | Eligible for self-certification |
|---|---|---|---|
| System testing report | 65% | 30 hours | Yes (extension) |

A project aimed at providing a response to a fictional corporate cyber security problem.

### Assessment group R

| | Weighting | Study time | Eligible for self-certification |
|---|---|---|---|
| Coursework | 100% | | No |

Analysis, evaluation, and modelling of a recent cyber-attack represented within a report aimed at given stakeholders

### Feedback on assessment

Via Tabula

---

## Availability

## Courses

This module is Core for:

- UWMA-H651 Undergraduate Cyber Security
  - Year 1 of H651 Cyber Security
  - Year 1 of H651 Cyber Security
  - Year 1 of H651 Cyber Security