

WM3B4-18 Operational Security Management

21/22

Department

WMG

Level

Undergraduate Level 3

Module leader

Tony Green

Credit value

18

Module duration

30 weeks

Assessment

100% coursework

Study location

University of Warwick main campus, Coventry

Description

Introductory description

This module draws together material, developed in detail in other modules, and presents the various interacting topics in an operational context. The focus is on operational security management relating to the cyber domain: maximising the benefits that flow from cyber engagement, whilst minimising the harms, through deliberate, managed activity. Some of this activity is obvious and directly cyber related: crypto key management or firewall rule change-control for example. Some is less obvious and indirectly cyber related: HR protocols for joiners and leavers for example.

At its core, the module is concerned with systematically addressing threats, vulnerabilities and the negative consequences that obtain should a threat exploit a vulnerability in any organisation's day-to-day cyber engagement. In that sense it uses the vocabulary of risk management. It is however particularly concerned with the home team engaging in concrete patterns (which may be deliberately randomised to hide the pattern) of activity that anticipate and foil an adversary's activity.

Module aims

1 - Anticipate cyber behaviours, both deliberately adversarial and unintentionally inept, that would

undermine an organisation's viability.

2 - Critically evaluate the vulnerabilities of an organisation through active probing of its systems.

3 - Manage cyber resources to maintain an organisation's viability in the face of adversarial or unintentional threats.

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.

Secure Operations Management and Service Delivery

Cryptography

Network security

System security

Application security

Physical security

Vulnerability Assessment

Dependable/resilient/survivable systems

Learning outcomes

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

- Anticipate cyber behaviours, both deliberately adversarial and unintentionally inept, that would undermine an organisation's viability
- Critically evaluate the vulnerabilities of an organisation through active probing of its systems
- Manage cyber resources to maintain an organisation's viability in the face of adversarial or unintentional threats

Indicative reading list

Anderson, Ross J., "Security Engineering: A Guide to Building Dependable Distributed Systems", 2 Ed, John Wiley & Sons (2008)

Nathans, David, "Designing and Building a Security Operations Center", Syngress (2014)

Svensson, Robert, "From Hacking to Report Writing: An Introduction to Security and Penetration Testing", Apress (2016)

Subject specific skills

1 - Anticipate cyber behaviours, both deliberately adversarial and unintentionally inept, that would undermine an organisation's viability.

2 - Critically evaluate the vulnerabilities of an organisation through active probing of its systems.

3 - Manage cyber resources to maintain an organisation's viability in the face of adversarial or unintentional threats.

Transferable skills

critical thinking, problem solving

Study

Study time

Type	Required
Supervised practical classes	18 sessions of 2 hours (20%)
Private study	48 hours (27%)
Assessment	96 hours (53%)
Total	180 hours

Private study description

Lecture time falls within workshop time.

One third of independent study time is not directly contributing to assessment

Two thirds of independent study time is contributing to assessment

Costs

No further costs have been identified for this module.

Assessment

You do not need to pass all assessment components to pass the module.

Assessment group A1

	Weighting	Study time
Coursework	100%	96 hours

Feedback on assessment

Written feedback for each assignment

Verbal feedback during tutorial sessions

Solutions provided to 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