WM244-18 Information Security Management

22/23

Department
WMG
Level
Undergraduate Level 2
Module leader
Harjinder Lallie
Credit value
18
Module duration
30 weeks
Assessment
Multiple
Study location
University of Warwick main campus, Coventry

Description

Introductory description

All organisations have information that they value and that value needs protecting. Within an organisation, some individuals carry formal responsibility for protecting the value of information. Ensuring that the responsible persons within an organisation have appropriate confidence in the security measures, which are protecting the organisation's valuable information, is the realm of information security management.

Why the organisation might value the information will vary from organisation to organisation and from information point to information point. The properties of the information that give it value similarly will vary by organisation and by information point. Some information will be special secret knowledge that gives the organisation competitive advantage; if that information leaks to a competitor, then its value is reduced. Some information may control the organisation's processes; if this controlling information is changed, then its value may be reduced since it causes the organisation to behave less well. Some information may relate to external perception of the organisation's ability to function; if external parties perceive this publicity information is not under the control of the organisation, then future opportunities for the organisation may be degraded through loss of trust.

Determining the relationship between the properties of information that give it value, the

vulnerability of those properties to degradation, threats that might take advantage of the vulnerability to degradation, and the resultant impact to the organisation when bad things happen, is the realm of information risk management. Things can be done to reduce the vulnerability, the threat, or the severity of the impact. These things enhance information security.

Information security management should give those with responsibility for information security, the confidence that things protecting information security are doing what they should. It is about having the strategy, policy, processes, behaviours, and technology, in place and coherently supporting each other.

Module aims

Adopt a responsible attitude to the social, ethical, legal and regulatory consequences that flow from professional engagement in security management.
Evaluate the overall coherence of an organisation's management of cyber security, recommending remediation where needed.

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.

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

Policy, Strategy, Awareness and Audit

Legal & Regulatory Environment

Learning outcomes

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

- Adopt a responsible attitude to the social, ethical, legal and regulatory consequences that flow from professional engagement in security management
- Evaluate the overall coherence of an organisation's management of cyber security, recommending remediation where needed

Indicative reading list

Campbell, Tony, “Practical Information Security Management: A Complete Guide to Planning and Implementation”, Apress (2016)

Landoll, Douglas J., “Information Security Policies, Procedures, and Standards”, Auerbach Publications (2016)

Yar, Majid, “Cybercrime and Society”, 2 Ed, Sage Publications Ltd. (2013)

View reading list on Talis Aspire

Subject specific skills

Adopt a responsible attitude to the social, ethical, legal and regulatory consequences that flow from professional engagement in security management.
Evaluate the overall coherence of an organisation's management of cyber security, recommending remediation where needed.

Transferable skills

Organisational awareness

Study

Study time

Type	Required
Supervised practical classes	18 sessions of 2 hours 30 minutes (25%)
Private study	45 hours (25%)
Assessment	90 hours (50%)
Total	180 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 do not need to pass all assessment components to pass the module.

Assessment group A3

	Weighting	Study time
Assignment 1	50%	45 hours
Assignment 2	50%	45 hours

Assessment group R1

	Weighting	Study time
Resubmission assignment	100%	

Feedback on assessment

Written feedback for each assignment
Verbal 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