WM088-15 Enterprise Cyber Security

24/25

Department
WMG
Level
Taught Postgraduate Level
Module leader
Christo Panchev
Credit value
15
Module duration
4 weeks
Assessment
Multiple
Study location
University of Warwick main campus, Coventry

Description

Introductory description

This module is effectively the capstone module of postgraduate cyber study, drawing together many aspects of the course. It has been developed in collaboration with a commercial partner of international standing to address key strategic cyber security issues from the perspective of an organisation's Chief Security Officer (CSO).

Topics to be addressed include communicating cyber issues to a board in terms that are relevant to them. Identity is addressed; especially the challenges that are associated with access control in a federated environment during times of transition such as during merger and acquisition. Trust is considered. The highly interconnected nature of Cyber-Physical systems are analysed to help provide a framework to reason about consequences (and their mitigation) in the face of cyber threat. Trends in cloud, analytics, mobile and social are looked at from the cyber perspective.

Module aims

The module equips students to take a broad-ranging view of cyber security in a manner, similar to that undertaken during large-scale cyber security consultancy.

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 strategic context setting of Cyber Security. The culture of cyber security, society, a day in the life of a CSO including how to explain cyber security issues to the board members;

Identity and Access Control. Theory of identity management vs real world, authentication factors, identity in a supply-chain, Federated identity management systems, NATO/coalition operations, Mergers and Acquisitions. Assured sharing frameworks.

Professionalism. The insider threat, legal, ethical, cultural and diversity.

Trustworthiness, and Risk Framework. Trust vs Risk; Agent systems and establishing trust for systems; case studies where security, safety, availability, resilience and/or dependability breaks down

Cyber Physical Systems. Utility and Smart Meter; Cascade failures; The impact of the merger of automation, human and electronics. For example, autonomous vehicles

Cloud, Analytics, Mobile, Social (CAMS). Wearable/ implanted devices; Historic Vs Future Trends

Each topic will normally be introduced through an exploration of the theoretical foundations and current research together with practical applications of the tools and techniques associated with the topics. Case studies will be used within the module to apply topics to a unifying application domain such as smart buildings, transport or the smart environment for an enterprise.

Learning outcomes

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

- Analyse and identify organisational cyber security imperatives
- Articulate organisational cyber security imperatives to key decision makers in an organisation
- Recommend actions to address organisational cyber risk exposure
- Develop a rigorous and convincing action plan/narrative to address organisational cyber risk exposure.

Indicative reading list

Hubbard, D; The Failure of Risk Management (2009)
Anderson, R;Security Engineering (2008),
PAS 754:2014 Software Trustworthiness. Governance and management. Specification (2014), BSI
Intelligent Buildings: Understanding and managing the security risks (2014), IET
CPNI, Holistic Management of Employee Risk (2012)
Corcoran, M; The Global Cyber Game (2013)

Subject specific skills

View cyber security from the cyber security consultant's perspective.

Transferable skills

Teamwork and working effectively with others, professionalism, organisational awareness

---

Study

Study time

Type	Required
Supervised practical classes	30 sessions of 1 hour (20%)
Private study	60 hours (40%)
Assessment	60 hours (40%)
Total	150 hours

Private study description

Further practical lab work and research.

Costs

No further costs have been identified for this module.

Assessment

You must pass all assessment components to pass the module.

Assessment group A2

	Weighting	Study time
Coursework	100%	60 hours

Report typically addressing a specific scenario. Example scenarios include the introduction of new technology, e.g. IoT devices within a medical setting. Participants may be asked to assess the risk associated with the introduction of the technology and propose recommendations in the form of an executive summary from a cyber security perspective addressed to senior high level executives who do not require a highly technical report and a section aimed at a CISO, who has the necessary technical background.

Assessment group R1

	Weighting	Study time
Coursework	100%	

A similar coursework to the original in terms of requirements, however, the scenario will be altered.

Feedback on assessment

Written feedback provided with the mark via tabula.

Availability

Anti-requisite modules

If you take this module, you cannot also take:

- WM088-10 Enterprise Cyber Security

Courses

This module is Core optional for:

- Year 1 of TWMS-H1S1 Postgraduate Taught Cyber Security Engineering (Full-time)