***CMT116: Cyber Security and Risk Management***

|  |  |
| --- | --- |
| **School** | Cardiff School of Computer Science and Informatics |
| **Department Code** | COMSC |
| **Module Code** | CMT116 |
| **External Subject Code** | 100366 |
| **Number of Credits** | 20 |
| **Level** | L7 |
| **Language of Delivery** | English |
| **Module Leader** | Dr Martin Chorley |
| **Semester** | Autumn Semester |
| **Academic Year** | 2019/0 |

**Outline Description of Module**

This module aims to provide students with a systematic understanding of cyber security management, and of risk assessment and management, and with the skills to critically analyse and, evaluate existing practices. The module covers key cyber security concepts, principles, technologies and practices. The module delivers hands-on experience of conducting risk assessment for an information system, threat modelling, developing security policies of different types and strategy for an organisation. This module enables students to practice the skills of communicating security concepts and needs to a wide range of audiences; applying common security frameworks and best practices, as well as evaluating their effectiveness; researching and analysing recent cyber security incidents, threats and vulnerabilities. The module informs students about legal and regulatory environment surrounding the development and use of Information and Communication Technology (ICT) and information systems, as well as about ethics and responsibilities of cyber security professionals.

**On completion of the module a student should be able to**

1. Determine, establish and maintain appropriate information security governance within an organisation
2. Identify, analyse, evaluate and manage risks related to different components of an information system (i.e. data, people, processes, hardware, software and network) accounting for current threat landscape
3. Identify and effectively articulate different types of threat to, and vulnerabilities of, information systems to a range of audiences (e.g. top management, end users, non-technical and technical experts)
4. Critically analyse a wide range of security countermeasures, select and justify appropriate security countermeasures to mitigate risks in an information system
5. Apply popular risk assessment methodologies to a case studies (e.g. Octave Allegro, STRIDE, DREAD)
6. Define and implement effective security policies and processes within an organisation, make and sustain argument; make judgement and propose solutions
7. Effectively use common information security management frameworks (e.g. ISO/IEC 27000, COBIT, NIST)
8. Be aware of the current computer misuse, data protection, copyright and privacy legislation, as well as security ICT regulations and guidelines, including GDPR
9. Evaluate and calculate return of security investments and economic impact of a security-related incident on business

**How the module will be delivered**

The module will be delivered as a combination of theoretical and practical interactive contact sessions, which will include discussions, tutorial, individual and group practical exercises inspired by a problem-based learning approach. The module will use a range of standards and common security management frameworks, practical guides for risk assessment methodologies and case studies as learning material. Three information security experts (internal and external) will be invited to present to student on the topics of risk assessment, information security management in a large organisation, and new cyber security threats and vulnerabilities. The students will also be provided with additional reading and self-study material.

**Skills that will be practised and developed**

Application of common security frameworks to case studies

Estimating the impact of security incidents on business

Analysis of organisation’s security strategy and policy

Security policy development

Calculating return on security investments

Communicating security risks

Establishing the context for risk assessment

Risk identification, estimation, evaluation

Choice of appropriate security control(s)

Risk monitoring and review

Critical analysis of an evidence-base available to a security professional

Derivation of appropriate professional, ethical requirements for security professionals

Evaluating the effectiveness of security countermeasures

Research a range of cyber security threats and vulnerabilities

Critically assess the challenges of information security and risk management

Present arguments that evidence understanding of the subject

Professionalism in the workplace

Transferable Skills (Listening, Communication, Time Management, Research, Literature Review and Analysis, Group Work, Reflective Thinking and Learning, Report Writing, Critical Thinking, Rhetoric and Argumentation)

**How the module will be assessed**

There will be **two**points of assessment in this module.

A written assessment (3000 words) will test students’ ability to apply the theoretical material and methodologies learnt in the module to a specific case study, the ability to find, research and cranially analyse relevant information. The coursework will provide an opportunity to deepen and improve the knowledge gain during the contact hours. The assessment will be presented in the form of a portfolio combining a range of tasks and exercise that were addressed in the module, but independently applied by a student to a given case study. Students would need to make judgements and propose solutions, make argument and justify their solutions. (LO1-4, LO6)

A computerised test (1.5 hours) will assess students’ understanding of key cyber security and risks concepts, principles, as well as their knowledge of common security frameworks, standards and regulations, risk assessment and threat modelling methodologies. The test will assess the ability to calculate ROSI for given case studies. The test will include multiple-choice, fill-in the blank, matching and calculated numeric types of questions. Students with special provision will be given more time for completing the test as advised by the responsible department. (LO5, LO7, LO8, LO9).

*Students will be provided with reassessment opportunities in line with University regulations.*

**Assessment Breakdown**

| **Type** | **%** | **Title** | **Duration(hrs)** |
| --- | --- | --- | --- |
| Class Test | 30 | Computerised Test | N/A |
| Written Assessment | 70 | Cyber Security And Risk Management Portfolio | N/A |

**Syllabus content**

**Introduction to cyber security and risk management**

* Key concepts and terminology (Risk, Threat, Vulnerability, Asset, Impact, Security Goals, Security Countermeasures)
* Security fundamentals and core principles
* Common security frameworks
* Cyber security governance
* Case studies/scenarios

**Risk Assessment and Management**

* Risk Assessment Methodologies and Frameworks (ISO/IEC 27005, NIST SP 800-30, CESG Information Assurance Standards, STRIDE, DREAD, OCTAVE Allegro, COBIT 5)
* Understanding and quantifying risk (likelihood, severity, impact)
* Selection of appropriate controls (cost-effectiveness)
* Asset management (ISO 55001:2014)

**Security Economics**

* Security economics

Return on security investments (ROSI)

Consequences of a security incident on business

* Measuring security. Security metrics

**Business and Cyber Security**

* Security as a business-enabler
* Security strategy and alignment with business objectives (ITIL)
* Role of top management
* Security culture
* Roles and responsibilities
* A hierarchy of security policies. Role and function of a security policy.
* Internal and external audit
* Cloud security (Cloud Security Alliance).

**Threat Modelling**

* Threat landscape
* Adversarial thinking and motivation of cyber attacks
* Threat Modelling Methodologies
* Attack- and fault-trees
* Goal-oriented risk assessment

**Regulations, Ethical and Professional Issues**

* Ethics and professionalism in Information Security domain
* Professional certification
* Managing security in the workplace
* Security education and awareness
* Current legal and regulatory environment (inc. GDPR, PCI DSS, NIS)

**Essential Reading and Resource List**

* National Cyber Security Centre Guidance <https://www.ncsc.gov.uk/guidance>
* BS EN ISO/IEC 27000:2017 - Information technology — Security techniques — Information security management systems — Overview and vocabulary
* BS EN ISO/IEC 27001:2017 - Information technology. Security techniques. Information security management systems. Requirements
* BS EN ISO/IEC 27002:2017 - Information technology. Security techniques. Code of practice for information security controls
* BS EN ISO/IEC 27005:2017 - Information technology. Security techniques. – Information Security Risk Management
* ISO 31000:2009 – Risk Management
* NIST Special Publication 800-30 - Information Security. Guide for Conducting Risk Assessments

**Background Reading and Resource List**

·Risk Analysis and Security Countermeasure Selection, Second Edition. Thomas L. Norman. 2015

·Cyber Security Management: A Governance, Risk and Compliance Framework. First Edition. P. Trim,‎ Yang-Im Lee.

·Security Engineering. Second Edition. Ross Anderson. 2008

·Professional Issues in Information Technology, F Bott, BCS, 2005.

·Ethics for the Information Age, M J Quinn, Pearson Education, 4th ed., 2011.

In addition, students will be expected to widely research related topics issues in appropriate academic journals, professional magazines and press.

[**Copyright Cardiff University.**](http://www.cardiff.ac.uk/legals/copyright.html)**Registered charity no. 1136855**