CS3190 Information Security

Level: 3 **Credits: 10** **Teaching Period: 1** **Module Tutor: Mr BS Doherty**

Aims

To provide computing or closely related subject undergraduates with deeper knowledge, advanced skills and understanding to allow them to contribute to development, design, evaluation and management of information security, using appropriate technologies, techniques, and procedures and with awareness of legal and social contexts.

Content

Concepts and definitions: The need for and benefit of information security. Threats to information systems, both malicious and non-malicious.
Methods: Protection, detection and reaction Access control security Identity management, security policy and standards. Encryption, identification and authentication.
Human factors. Biometrics. Disaster recovery. Intrusion prevention.
Legal, standards and ethical aspects: Legal framework. Security standards and procedures. Principles of conduct. Privacy
Managing information security: Information security risk analysis and risk assessment. Probability, risk analysis, the risk matrix. Controls. Business continuity management
Applications: Copyright Protection; E-commerce and e-cash; communication. Distributed systems security
Crime: Information warfare and cyber terrorism; Financial crime; Forensic Computing

Teaching

Lectures: 22 hours; Lab classes: 4 hours; Self-study project: 10 hours.

Assessment

Written exam: 80% (2 hours, January)
Practical assignment: 20%

Module outcomes

What the student should gain from successful completion of the module	*Teaching/Learning Methods*	*Assessment Methods*
Knowledge and Understanding		
Common information hazards; computer crime Operation and limitations of common information safeguards Framework for and management of information security Ethics, privacy, and organisational information Laws, codes of practice, and standards	Lectures, literature and lab-based projects, supported by self-study using other materials and online resources.	Exam, coursework
Intellectual Skills		
Design of organisational policies for information security and privacy Creating threat scenarios for particular systems and situations Specification of safeguards for computer-based information assets Planning and organising of information security functions Analysing information risks and choosing organisational responses	Lectures, coursework, literature study, tutorial problems	Exam, coursework
Professional/Subject-Specific Skills		
Analyse, design, build and evaluate information security Evaluate and select appropriate technologies and tools Critically evaluate new and emerging techniques and information technologies for full awareness of the security ramifications	Lectures, lab classes, coursework, tutorial problems	Coursework; application to exam scenarios
Transferable Skills		
Abstract significant information from unstructured sources at a level sufficient to keep up to date and communicate with computing professionals Demonstrate research skills and make effective use of various sources	Reading beyond lectures; coursework projects	Coursework; interpretation of exam scenarios

Learning resources

Charles Pfleeger & Shari Pfleeger, Security in Computing (3rd edition), Prentice-Hall, 2002
Bruce Schneier, Secrets and Lies: Digital Security in a Networked World, Wiley, 2000
Ross Anderson, Security Engineering: Building Dependable Distributed Systems, Wiley, 2001
Dieter Gollman, Computer Security, Wiley, 1998

Other study requirements to take this module

CS1240 or CS1280 Internet Computing
CS1410 Java Program Dvelopment or CS2300 Java Program Construction