MODULE DESCRIPTOR

TITLE	ELECTRONIC CRIME			
SI MODULE CODE	44-5961-00L			
CREDITS	20			
LEVEL	5			
JACS CODE	G500 - Information Systems			
SUBJECT GROUP	BUSINESS OPERATIONS AND SYSTEMS - SBS			
DEPARTMENT	Management			
MODULE LEADER	Lucian Tipi			
NOTIONAL STUDY HOURS BY TYPE	Tutor-led	Tutor-directed	Self-directed	Total Hours
	36	72	92	200

MODULE AIM(S)

- Appreciation of the history and developments in electronic crime in an international context

- Identify the threats and vulnerabilities existing within organisational Information Systems.

- Understand and assess the impact on organisations and individuals of the major types of electronic crime.

- Assess the protection and assurances available to organisations and individuals to avoid becoming victims of electronic crime as well as to respond to such crime.

MODULE LEARNING OUTCOMES

By engaging successfully with this module a student will be able to

On completion of the module you will be able to:

1. Assess the vulnerabilities within contemporary Information Systems.
2. Identify and assess the threats posed by the major types of electronic crime.
3. Appreciate and evaluate risk management processes necessary for Information Systems and best practice in Information Systems security.
4. Assess and evaluate the stages of digital forensic investigation.
5. Understand and evaluate the protection offered by technology and legislation when tackling Information Systems security and electronic crime.

INDICATIVE CONTENT

These are examples of the content of the module

The module will cover a broad range of topics in the very fast moving area of Electronic Crime. An indicative list of topics can be found in the following:

- History and developments of electronic crime, e.g. malware, denial of service and distributed denial of service, hacking, spyware, etc.

- Vulnerabilities of and threats to Information Systems within organisations, the commercial use of the Internet, Information Systems infrastructure
- Frameworks for classifying electronic crime
- Legislation and associated cases
- Government and commercial initiatives for Information Systems governance and security
- Digital forensics and electronic evidence
- Software applications for digital forensics

This is not an exhaustive list; other topics/issues will be discussed during the module with relevant examples presented as they will be identified during the running of the module. Relevant current case studies will be utilised as appropriate.

LEARNING AND TEACHING METHODS

Students will be supported in their learning, to achieve the above outcomes, in the following ways

Lectures and Seminars

The module will be delivered by a series of sessions which will have a lecture element followed by a seminar element – so called “lectorial” sessions. Also the sessions will contain a significant element of student led discussions. The lecture element will deliver the core theoretical material of the module and this will be then augmented with case studies, examples and activities in the seminar element.

Some of the module sessions will be student led and will be based on discussions, case studies and analysis of topical cases; the seminars will explore topical issues related to the core material of the module as well as the assessment package of the module.

A series of student led presentations based on research into key topics will be a feature of the sessions. Oral formative feedback will be provided at the end of the presentations, to prepare students for their coursework.

There is an intention to bring in guest speakers as appropriate. A number of drop in sessions will be run in order to provide support with the coursework.

Virtual Learning Environment (VLE) - Blackboard

The module has a dedicated Blackboard site which students are expected to access on a regular basis. The Blackboard site is used to communicate information to students outside of contact sessions (via the 'Announcements' page). In addition, the blackboard site includes:

- An electronic version of the module handbook
- Links to lecture/PowerPoint slides
- Details regarding assessments
- Seminar exercises
- Wikis to enable one to one communication with the students and the provision of formative feedback
- Case studies utilised throughout the module
- Additional topical and contemporary information with direct links to external websites.
- Staff contact details

ASSESSMENT STRATEGY AND METHODS

Assessment will involve course work and an examination. The Coursework, an individual written assessment, will be an evaluation piece on a topic that will be decided following the discussions between the module leader and the students. A choice of several topics will be given to students and then based on the in sessions discussions a topic will be chosen. All students will then need to work on the chosen topic.

You will have the opportunity to test and evaluate your learning through formative and summative assessment. A variety of assessment methods will be used and time will be allocated for staff and students to work through their expectations and understanding of the module's assessment tasks.

Task No.	Task Description	Task Type	Task Weighting %	Word Count / Duration	In-module retrieval available
1	Individual Written Coursework	Coursework	60	3000 words	No
2	Examination	Examination	40	2 hours	No

ASSESSMENT CRITERIA

The assessment grid for the module is presented below:

Individual Written Assignment Learning Outcome	Fail	Pass	2.2	2.1	First
1	The vulnerabilities area is not assessed appropriately or is presented and evaluated at an insufficient level.	The vulnerabilities area is assessed, presented, evaluated and analysed at a sufficient level.	The vulnerabilities area is assessed, presented, evaluated and analysed at an appropriate level.	The vulnerabilities area is assessed, presented, evaluated and analysed at a good level.	The vulnerabilities area is assessed, presented, evaluated and analysed at an excellent level. Originality is being shown.
2	No, very little or biased assessment of the threats posed by the major types of electronic crime.	Sufficient assessment of the threats posed by the major types of electronic crime.	Appropriate assessment of the threats posed by the major types of electronic crime.	Good assessment of the threats posed by the major types of electronic crime.	Excellent assessment of the threats posed by the major types of electronic crime.
3	Insufficient analysis of the risk management processes and insufficiently evidenced best practice in IS security.	Sufficient analysis of the risk management processes and sufficiently evidenced best practice in IS security.	Appropriate analysis of the risk management processes and appropriately evidenced best practice in IS security.	Good analysis of the risk management processes and well evidenced best practice in IS security.	Excellent analysis of the risk management processes and very well evidenced best practice in IS security. Future issues explored.
4	A poor evaluation of the stages of digital forensic investigation.	A sufficient evaluation of the stages of digital forensic investigation.	An appropriate evaluation of the stages of digital forensic investigation.	A good evaluation of the stages of digital forensic investigation.	An excellent evaluation of the stages of digital forensic investigation. Legal and technical complications are presented and discussed.
5	Insufficient analysis of the protection offered by technology and insufficient analysis of the legislative framework.	Sufficient analysis of the protection offered by technology and sufficient analysis of the legislative framework.	Appropriate analysis of the protection offered by technology and appropriate analysis of the legislative framework.	Good analysis of the protection offered by technology and good analysis of the legislative framework.	Excellent analysis of the protection offered by technology and excellent analysis of the legislative framework. Future challenges related to technology protection and legislation explored.

FEEDBACK

Students will receive feedback on their performance in the following ways

Both formative and summative feedback will be provided to students as follows:

Formative feedback:

- Formative feedback will be provided by the teaching team on an on-going basis throughout the duration of the module. The module Blackboard site will be used as one of the vehicles for this.
- At least one session per semester during the delivery of the module will be dedicated to providing formative feedback to students in its entirety. These will take the form of drop in style sessions.
- Students will be encouraged throughout the delivery of the module to seek clarifications on the topics being presented and to raise their own discussion points – the ensuing discussions with the tutor and the rest of the class will also form an important part of the formative feedback given to students.

Summative feedback:

- Written feedback following the submission of Assessment Task 1 will be made available by the module team.
- Summative feedback will also be available following Assessment Task 2, the examination, in the form of the marks awarded. Students will also be provided with opportunities for individual feedback.

LEARNING RESOURCES (INCLUDING READING LISTS)

The module leader liaises closely with the university learning centre to ensure a wide variety of the latest books and articles are available to aid your studies. Students will also be able to utilise the online journals database via the learning centre website. The module guide will outline key readings along with utilising the Talis reading list system.

Due to the very fast moving nature of the issues approached in the module, the reading list will be frequently updated, from one delivery of the module to another. Although an extensive reading list is provided, students are not expected to read all of the materials provided, but rather to select a range of titles that are appropriate.

Students will need to make extensive use of web resources, particularly when it comes to finding relevant case studies needed to support their discussion.

Electronic copies of all teaching materials will be placed on Blackboard along with sample assessments, formative work, weblinks and additional resources. A discussion board will be available so that you are able to communicate with your fellow students and tutors.

Recommended Texts:

Laudon and Laudon; Management Information Systems

Dhillon G.; Principles of Information Systems Security: Texts and Cases

Kenneth C. Laudon and Carol Guercio Traver; E-Commerce 2010: International Version: Business, Technology, Society

Austin R. and Darby C. A. R.; The Myth of Secure Computing; Harvard Business Review

Portnoy M. and Goodman S.; Global Initiatives to Secure Cyberspace: An Emerging Landscape (Advances in Information Security)

Khalfan S.; Managing internal and external risk in the information age

Coderre D.; Computer Aided Fraud Prevention and Detection: A Step by Step Guide

Web Resources

http://www.zdnet.com

http://www.getsafeonline.org

http://www.itgovernance.co.uk

http://www.bis.gov.uk/policies/business-sectors/information-security

http://www.bbc.co.uk/news

SECTION 2 'MODEL A' MODULE (INFORMATION FOR STAFF ONLY)

MODULE DELIVERY AND ASSESSMENT MANAGEMENT INFORMATION

MODULE STATUS - INDICATE IF ANY CHANGES BEING MADE

NEW MODULE	No
EXISTING MODULE - NO CHANGE	No
Title Change	No
Level Change	No
Credit Change	No
Assessment Pattern Change	Yes
Change to Delivery Pattern	No
Date the changes (or new module) will be implemented	02/Sep/2013

MODULE DELIVERY PATTERN

Module Begins	Module Ends
08/Aug/2011	15/Apr/2012
17/Sep/2012	30/May/2012

Is timetabled contact time required for this module?	Yes

Are any staff teaching on this module non-SHU employees?	No

MODULE ASSESSMENT INFORMATION

Does the Module Require Either	
Overall Percentage Mark of 40%	Yes
Overall Pass / Fail Grade	No

FINAL TASK

According to the Assessment Strategy shown in the Module Descriptor, which task will be the LAST TASK to be taken or handed-in? (Give task number as shown in the Assessment Strategy)	Task No. 2

MODULE REFERRAL STRATEGY

Task for Task (as shown for initial assessment strategy)	Yes
Single Referral Package for All Referred Students	No

REVISIONS

Date	Reason
July 2012	Assessment Framework review