### INFORMATION SECURITY GROUP

#### Course Specification 2016-17

<table>
<thead>
<tr>
<th>Code:</th>
<th>IY5605</th>
<th>Course Value:</th>
<th>20</th>
<th>Status:</th>
<th>Option</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Title:</th>
<th>Cyber Crime</th>
<th>Availability:</th>
<th>Spring Term</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Prerequisites:</th>
<th>Core courses</th>
<th>Recommended:</th>
<th>None</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Co-ordinator:</th>
<th>Martin Warren</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Co-course Staff:</th>
<th>Martin Warren</th>
</tr>
</thead>
</table>

### Aims:
- complement other information security courses by examining the subject from the criminal angle
- investigate the history and causes of cyber crime
- examine the effects of cyber crime through the experiences of victims and law enforcement
- consider the technologies that stand behind certain cyber crimes, namely malware (viruses, worms, Trojan Horses, etc.), email spamming and denial of service (DoS) attacks
- consider how to handle a digital crime scene

### Learning Outcomes:
- On successful completion of the course students will be able to:
  - identify and evaluate trends in cyber crime
  - relate computer security methodologies to criminal methods
  - detect criminal activity in a computerized environment
  - apply the criminal and civil law to computer criminality
  - explain how malware and other technical hacking techniques are used by criminals
  - understand the mechanisms hackers use to social engineer their victims
  - assess the mechanisms used to launch DoS and distributed DoS attacks and propose suitable countermeasures
  - compare and evaluate the views and responses of business, governments, and the media to cyber crime.

### Course Content:
- Introduction: Types of cyber crime, history, surveys, statistics and global connections
- Legal Measures: Computer Misuse, Criminal Damage, Copyright, Forgery, Fraud, Blackmail, Bribery & Investigative Powers
- Case Studies: Investigations into hacking, cases and misuse
- Social Engineering
- Fraud, Spam, Phishing and Pharming
- Malware: The types, effects, and investigations
- DoS and Distributed DoS: The causes, mechanisms, case studies, and countermeasures
- Network Crimes: Hacking methodologies via the Internet and attacks to other networks
- Content crime: Stalking, pornography, harassment & malicious communications
- The Future: The expansion of the Internet, pornography and other unsuitable material.
- Digital Evidence

### Teaching & Learning Methods:
Eleven 3-hour presentations with handouts and additional press material, and web references.

### Key Bibliography:
- Lloyd, I, Information Technology Law, Oxford University Press
- Blackstone's Statutes on IT and E-Commerce, Oxford University Press.
- Various web-sites including Sans Newsbytes and Sophos Naked Security.

### Formative Assessment and Feedback:
Two assignments are given during which cyber crime scenarios are discussed from an examination perspective. Also, tutorial sessions are used to provide feedback on student answers to exercise sheets.

### Summative Assessment:
**Exam** 100(%) This course is assessed solely by written examination consisting of a two-hour exam. (3 out 5 questions)
**Coursework** 0(%) Coursework does not contribute to the final assessment for this course.

### Deadlines:
The written examination will be held in the Summer term.

---

The information contained in this course outline is correct at the time of publication, but may be subject to change as part of the Department’s policy of continuous improvement and development. Every effort will be made to notify you of any such changes.