PICT840

Cyber Crime

S2 Evening 2017

Department of Security Studies and Criminology

Contents

General Information

Unit convenor and teaching staff
Angela Irwin
angela.irwin@mq.edu.au

Yves-Heng Lim
yves-heng.lim@mq.edu.au

Credit points
4

Prerequisites
Admission to MCRIM or MPICT or MCPICT or PGDipPICT or GradDipPICT or GradDipCPICT or PGCertPICT or GradCertPICT or GradCertCPICT or MPICTMIntSecSt or MCPICTMIntSecSt or MIntSecStud or PGDipIntSecStud or GradDipIntSecStud or PGCertIntSecStud or MCompForens or PGDipCompForens or PGCertCompForens or MInfoTech

Corequisites

Co-badged status

Unit description
Cybercrime refers to an array of criminal activity including offences against computer data and systems, computer-related offences, content offences, and copyright offences. While early computer hackers were more interested in youthful exploration, modern cybercrime is increasingly about criminal profit and this is reflected in the involvement of transnational organised crime groups. This unit will explore the types of cybercrime, the perpetrators, and investigation techniques.

Important Academic Dates

Information about important academic dates including deadlines for withdrawing from units are available at https://www.mq.edu.au/study/calendar-of-dates

Learning Outcomes

On successful completion of this unit, you will be able to:

Understand, analyse, and critically discuss different types of cyber crime activities with respect to the motivations, methods of operation of offenders, and the types of victims/ targets.

Demonstrate a comprehensive understanding of past, current cyber threats and future

trends in high tech crime.

Analyse the impact of cyber crime on government, businesses, society and individuals.

Demonstrate knowledge of relevant theories, cross disciplinary approaches (criminology and information security), and the applicability to the study of cyber crime.

Demonstrate a comprehensive understanding of strategies and steps to investigate digital evidence.

Assessment Tasks

Name	Weighting	Hurdle	Due
Participation/ engagement	10%	No	Weekly
Critical Review	10%	No	Week 3 and Week 8
Quizzes	20%	No	Week 4 and Week 9
Problem Based Learning	20%	No	Week 10
Major essay	40%	No	Week 11

Participation/ engagement

Due: **Weekly**
Weighting: **10%**

This will encourage students to engage critically in both classroom and online discussions. A variety of different activities will occur each week and students should be prepared to fully participate in these activities. This will include an online discussion for external students, and weekly seminar participation and attendance only for internal students). Please note that if an internal student is unable to attend a seminar they will be required to participate in the online discussion.

Online discussion format: at least one question will be posted to the discussion forum each week. Responses to each question should be a minimum of 100 words in length. Your postings to the online discussions should reflect your understanding and ability to synthesise course readings and seminar content, and to include related thoughts and analysis.

Your postings should advance the group's discussion of ideas and meanings about the material. Some ways you can further discussions include:

- expressing ideas or observations - where possible support them by more than personal opinion or anecdotal evidence;
- making a connection between the current discussion and previous discussion, using personal experience or readings
- commenting on or expanding another student’s statement;

- posting a substantive question aimed at furthering the group's understanding.

Please keep your posts brief, one or two paragraphs is sufficient. If citing course readings, in text references are sufficient.

For a posting to be counted for a given week, it must be entered by midnight on the Sunday of that week's activity. If entered later than this, the posting will not be counted.

A mark for the discussions will be awarded on the basis of:

- For internal students, your attendance and participation in the class (50%), and the content of your contribution (50%).
- For external students, your participation the online discussion (50%), and the content of your contribution (50%).

In assessing your contributions the following categories will be used:

- Level 1 - Postings providing a single point of view;
- Level 2 - Postings which make reference to other contexts or course material;
- Level 3 - Postings which offer a critical reflection on theoretical perspectives and/or practical experiences.

On successful completion you will be able to:

- Understand, analyse, and critically discuss different types of cyber crime activities with respect to the motivations, methods of operation of offenders, and the types of victims/ targets.
- Demonstrate a comprehensive understanding of past, current cyber threats and future trends in high tech crime.
- Analyse the impact of cyber crime on government, businesses, society and individuals.
- Demonstrate knowledge of relevant theories, cross disciplinary approaches (criminology and information security), and the applicability to the study of cyber crime.
- Demonstrate a comprehensive understanding of strategies and steps to investigate digital evidence.

Critical Review

Due: **Week 3 and Week 8**
Weighting: **10%**

Preparation of a 600 words critical review in Weeks 3 and 8 of one relevant article in the corresponding week is intended to encourage independent research and demonstrate a capacity to find, synthesise and critically evaluate information relevant to specific topics or issues. The critical review should demonstrate understanding of the key arguments of the article and critical evaluation of the article's merits (strengths/weaknesses).

A detailed marking matrix is available to all enrolled students on the unit ilearn site. Marking criteria in the marking matrix includes evaluation of the critical review.

On successful completion you will be able to:

- Understand, analyse, and critically discuss different types of cyber crime activities with respect to the motivations, methods of operation of offenders, and the types of victims/ targets.
- Demonstrate a comprehensive understanding of past, current cyber threats and future trends in high tech crime.
- Analyse the impact of cyber crime on government, businesses, society and individuals.
- Demonstrate a comprehensive understanding of strategies and steps to investigate digital evidence.

Quizzes

Due: **Week 4 and Week 9**
Weighting: **20%**

Two quizzes during the course will be in Week 4 and Week 9. The quizzes will be based around the readings, online resources, and course materials from specified weeks. The quizzes are intended to give students an opportunity to explore in details the issues covered in the unit and to develop a deeper understanding of the subject matter. Each quiz will be a total of one hour of T/F, multiple-choice, short answers, etc. Each quiz will be worth 10% of the overall grade available for the unit.

Internal students: In class quiz, the quiz is held in the tutorial time.

External students: The online quizzes, the quizzes, once released will be available 48 hours only and is open book. Students will have unlimited access to the quiz and may save their progress; however there will be only ONE chance for submission.

On successful completion you will be able to:

- Understand, analyse, and critically discuss different types of cyber crime activities with respect to the motivations, methods of operation of offenders, and the types of victims/ targets.
- Demonstrate a comprehensive understanding of past, current cyber threats and future trends in high tech crime.
- Analyse the impact of cyber crime on government, businesses, society and individuals.
- Demonstrate a comprehensive understanding of strategies and steps to investigate digital evidence.

Problem Based Learning

Due: **Week 10**
Weighting: **20%**

Objective

Problem based learning (PBL) Presentation in seminars of 30 minutes duration plus Q&A. The aim of this exercise is for groups to undertake a series of in-depth investigations into contemporary related topics. The presentation will cover the content provided in all the learning outcomes. Students will discuss and present on a specific research problem and incorporate the content provided in lectures and reading. The PBL reinforces critical thinking skills.

Requirements

Internal students: Students are required to form small groups at the beginning of the course. One presentations will be required for each group. Each group is required to (a) develop a written presentation in the form of PowerPoint slides (or equivalent) and (b) to make an oral presentation using these slides.

External students: Students are required to work as individuals. Students are required to submit a PowerPoint Presentation (or equivalent) with presenters' notes that, if presented orally, would extend to around 30 minutes (approximately 20- 25 slides), and 1000-1500 words per presentation appropriately supported by Oxford style references as footnotes, one presentations will be required for each student. Please note: No oral presentation is required for this assessment task. Each slide should contain logical, clear and easily understood points that demonstrate understanding of the topic. The notes section of the presentation should discuss or argue the relevance of each of the bullet points in the body of the slide. This enables the lecturer/ tutor to assess your understanding of the topic. You should also place in the notes section the details of the references that you have used in each slide.

Assessment

Internal students: The content of the slides will comprise 15% of the overall 30% course mark. Each group member receives the same mark. The presentation of the slides will then comprise the remaining 15% of the overall course mark. Each group member will be assessed individually. Assessing presentations are compiled in a standard form. A detailed marking matrix is available to all enrolled students on the unit ilearn site. The marking guide is available to all enrolled students on the unit ilearn site, that will be used to assess the content and presentation. Groups should organize themselves in such a way that work is evenly distributed between members. To this end, each group member must present for approximately equal time per person.

External students: The content of the slides will comprise 30% of the overall course mark. The marking guide is available to all enrolled students on the unit ilearn site, that will be used to assess the content and presentation.

Length

Each presentation should last for 30 minutes including Q&A.

Dates

Internal students: Presentations will take place on Week 10, Week 11, and Week 12.

External students, for a presentation to be counted for a given week, it must be submitted by midnight on the Sunday of Week 10.

On successful completion you will be able to:

- Understand, analyse, and critically discuss different types of cyber crime activities with respect to the motivations, methods of operation of offenders, and the types of victims/ targets.
- Demonstrate a comprehensive understanding of past, current cyber threats and future trends in high tech crime.
- Analyse the impact of cyber crime on government, businesses, society and individuals.
- Demonstrate knowledge of relevant theories, cross disciplinary approaches (criminology and information security), and the applicability to the study of cyber crime.
- Demonstrate a comprehensive understanding of strategies and steps to investigate digital evidence.

Major essay

Due: **Week 11**
Weighting: **40%**

Students will choose a topic from a list of given topics, if students are not writing an essay from the given topics, you must seek approval from your instructor on your essay question in the first instance. The essay length is 3000 words including bibliography, but not footnotes and footnoted references, or title page. The essay will show student's knowledge of theories and practice and their ability to critically evaluate the chosen topic.

On successful completion you will be able to:

- Understand, analyse, and critically discuss different types of cyber crime activities with respect to the motivations, methods of operation of offenders, and the types of victims/ targets.
- Demonstrate a comprehensive understanding of past, current cyber threats and future trends in high tech crime.
- Analyse the impact of cyber crime on government, businesses, society and individuals.
- Demonstrate knowledge of relevant theories, cross disciplinary approaches (criminology and information security), and the applicability to the study of cyber crime.
- Demonstrate a comprehensive understanding of strategies and steps to investigate digital evidence.

Delivery and Resources

UNIT REQUIREMENTS AND EXPECTATIONS

- You should spend an average of 12 hours per week on this unit. This includes listening to lectures prior to seminar or tutorial, reading weekly required materials as detailed in iLearn, participating in Ilearn discussion forums and preparing assessments.
- Internal students are expected to attend all seminar or tutorial sessions, and external students are expected to make significant contributions to on-line activities.
- In most cases students are required to attempt and submit all major assessment tasks in order to pass the unit.

REQUIRED READINGS

- The citations for all the required readings for this unit are available to enrolled students through the unit iLearn site, and at Macquarie University's library site. Electronic copies of required readings may be accessed through the library or will be made available by other means.

TECHNOLOGY USED AND REQUIRED

- Computer and internet access are essential for this unit. Basic computer skills and skills in word processing are also a requirement.
- This unit has an online presence. Login is via: https://ilearn.mq.edu.au/
- Students are required to have regular access to a computer and the internet. Mobile devices alone are not sufficient.
- Information about IT used at Macquarie University is available at http://students.mq.edu.au/it_services/

SUBMITTING ASSESSMENT TASKS

- All text-based assessment tasks are to be submitted, marked and returned electronically. This will only happen through the unit iLearn site.
- Assessment tasks must be submitted as a MS word document by the due date.
- Most assessment tasks will be subject to a 'TurnitIn' review as an automatic part of the submission process.
- The granting of extensions is subject to the university's Disruptions Policy. Extensions

will not in normal circumstances be granted by unit conveners or tutors, but must be lodged through Disruption to Study: http://www.students.mq.edu.au/student_admin/manage_your_study_program/disruption_to_studies/.

LATE SUBMISSION OF ASSESSMENT TASKS

- If an assignment is submitted late, 5% of the available mark will be deducted for each day (including weekends) the paper is late.
- For example, if a paper is worth 20 marks, 1 mark will be deducted from the grade given for each day that it is late (i.e. a student given 15/20 who submitted 4 days late will lose 4 marks = 11/20).
- The same principle applies if an extension is granted and the assignment is submitted later than the amended date.

WORD LIMITS FOR ASSESSMENT TASKS

- Stated word limits include footnotes and footnoted references, but not bibliography, or title page.
- Word limits can generally deviate by 10% either over or under the stated figure.
- If the number of words exceeds the limit by more than 10%, then penalties will apply. These penalties are 5% of the awarded mark for every 100 words over the word limit. If a paper is 300 words over, for instance, it will lose 3 x 5% = 15% of the total mark awarded for the assignment. This percentage is taken off the total mark, i.e. if a paper was graded at a credit (65%) and was 300 words over, it would be reduced by 15 marks to a pass (50%).
- The application of this penalty is at the discretion of the course convener.

REASSESSMENT OF ASSIGNMENTS DURING THE SEMESTER

- Macquarie University operates a Grade Appeal Policy in cases where students feel their work was graded inappropriately: http://www.mq.edu.au/policy/docs/gradeappeal/policy.html
- In accordance with the Grade Appeal Policy, individual works are not subject to regrading.

STAFF AVAILABILITY

- Department staff will endeavour to answer student enquiries in a timely manner. However, emails or iLearn messages will not usually be answered over the weekend or public holiday period.
- Students are encouraged to read the Unit Guide and look at instructions posted on the iLearn site before sending email requests to staff.

Policies and Procedures

Macquarie University policies and procedures are accessible from Policy Central. Students should be aware of the following policies in particular with regard to Learning and Teaching:

Academic Honesty Policy http://mq.edu.au/policy/docs/academic_honesty/policy.html

Assessment Policy http://mq.edu.au/policy/docs/assessment/policy_2016.html

Grade Appeal Policy http://mq.edu.au/policy/docs/gradeappeal/policy.html

Complaint Management Procedure for Students and Members of the Public http://www.mq.edu.au/policy/docs/complaint_management/procedure.html

Disruption to Studies Policy (in effect until Dec 4th, 2017): http://www.mq.edu.au/policy/docs/disruption_studies/policy.html

Special Consideration Policy (in effect from Dec 4th, 2017): https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policies/special-consideration

In addition, a number of other policies can be found in the Learning and Teaching Category of Policy Central.

Student Code of Conduct

Macquarie University students have a responsibility to be familiar with the Student Code of Conduct: https://students.mq.edu.au/support/student_conduct/

Results

Results shown in *iLearn*, or released directly by your Unit Convenor, are not confirmed as they are subject to final approval by the University. Once approved, final results will be sent to your student email address and will be made available in eStudent. For more information visit ask.mq.edu.au.

Student Support

Macquarie University provides a range of support services for students. For details, visit http://students.mq.edu.au/support/

Learning Skills

Learning Skills (mq.edu.au/learningskills) provides academic writing resources and study

strategies to improve your marks and take control of your study.

- Workshops
- StudyWise
- Academic Integrity Module for Students
- Ask a Learning Adviser

Student Services and Support

Students with a disability are encouraged to contact the Disability Service who can provide appropriate help with any issues that arise during their studies.

Student Enquiries

For all student enquiries, visit Student Connect at ask.mq.edu.au

IT Help

For help with University computer systems and technology, visit http://www.mq.edu.au/about_us/offices_and_units/information_technology/help/.

When using the University's IT, you must adhere to the Acceptable Use of IT Resources Policy. The policy applies to all who connect to the MQ network including students.

Graduate Capabilities

PG - Capable of Professional and Personal Judgment and Initiative

Our postgraduates will demonstrate a high standard of discernment and common sense in their professional and personal judgment. They will have the ability to make informed choices and decisions that reflect both the nature of their professional work and their personal perspectives.

This graduate capability is supported by:

Learning outcomes

- Understand, analyse, and critically discuss different types of cyber crime activities with respect to the motivations, methods of operation of offenders, and the types of victims/ targets.
- Demonstrate a comprehensive understanding of past, current cyber threats and future trends in high tech crime.
- Analyse the impact of cyber crime on government, businesses, society and individuals.
- Demonstrate knowledge of relevant theories, cross disciplinary approaches (criminology and information security), and the applicability to the study of cyber crime.
- Demonstrate a comprehensive understanding of strategies and steps to investigate digital evidence.

Assessment tasks

- Participation/ engagement
- Critical Review
- Problem Based Learning
- Major essay

PG - Discipline Knowledge and Skills

Our postgraduates will be able to demonstrate a significantly enhanced depth and breadth of knowledge, scholarly understanding, and specific subject content knowledge in their chosen fields.

This graduate capability is supported by:

Learning outcomes

- Understand, analyse, and critically discuss different types of cyber crime activities with respect to the motivations, methods of operation of offenders, and the types of victims/ targets.
- Demonstrate a comprehensive understanding of past, current cyber threats and future trends in high tech crime.
- Analyse the impact of cyber crime on government, businesses, society and individuals.
- Demonstrate knowledge of relevant theories, cross disciplinary approaches (criminology and information security), and the applicability to the study of cyber crime.
- Demonstrate a comprehensive understanding of strategies and steps to investigate digital evidence.

Assessment tasks

- Participation/ engagement
- Critical Review
- Quizzes
- Problem Based Learning
- Major essay

PG - Critical, Analytical and Integrative Thinking

Our postgraduates will be capable of utilising and reflecting on prior knowledge and experience, of applying higher level critical thinking skills, and of integrating and synthesising learning and knowledge from a range of sources and environments. A characteristic of this form of thinking is the generation of new, professionally oriented knowledge through personal or group-based critique of practice and theory.

This graduate capability is supported by:

Learning outcomes

- Understand, analyse, and critically discuss different types of cyber crime activities with respect to the motivations, methods of operation of offenders, and the types of victims/ targets.
- Demonstrate a comprehensive understanding of past, current cyber threats and future trends in high tech crime.
- Analyse the impact of cyber crime on government, businesses, society and individuals.
- Demonstrate knowledge of relevant theories, cross disciplinary approaches (criminology and information security), and the applicability to the study of cyber crime.
- Demonstrate a comprehensive understanding of strategies and steps to investigate digital evidence.

Assessment tasks

- Participation/ engagement
- Critical Review
- Quizzes
- Problem Based Learning
- Major essay

PG - Research and Problem Solving Capability

Our postgraduates will be capable of systematic enquiry; able to use research skills to create new knowledge that can be applied to real world issues, or contribute to a field of study or practice to enhance society. They will be capable of creative questioning, problem finding and problem solving.

This graduate capability is supported by:

Learning outcomes

- Understand, analyse, and critically discuss different types of cyber crime activities with respect to the motivations, methods of operation of offenders, and the types of victims/ targets.
- Demonstrate a comprehensive understanding of past, current cyber threats and future trends in high tech crime.
- Analyse the impact of cyber crime on government, businesses, society and individuals.
- Demonstrate knowledge of relevant theories, cross disciplinary approaches (criminology and information security), and the applicability to the study of cyber crime.
- Demonstrate a comprehensive understanding of strategies and steps to investigate digital evidence.

Assessment tasks

- Participation/ engagement
- Critical Review
- Quizzes
- Problem Based Learning
- Major essay

PG - Effective Communication

Our postgraduates will be able to communicate effectively and convey their views to different social, cultural, and professional audiences. They will be able to use a variety of technologically supported media to communicate with empathy using a range of written, spoken or visual formats.

This graduate capability is supported by:

Learning outcomes

- Understand, analyse, and critically discuss different types of cyber crime activities with respect to the motivations, methods of operation of offenders, and the types of victims/ targets.
- Demonstrate a comprehensive understanding of past, current cyber threats and future trends in high tech crime.
- Analyse the impact of cyber crime on government, businesses, society and individuals.
- Demonstrate knowledge of relevant theories, cross disciplinary approaches (criminology and information security), and the applicability to the study of cyber crime.
- Demonstrate a comprehensive understanding of strategies and steps to investigate digital evidence.

Assessment tasks

- Participation/ engagement
- Critical Review
- Quizzes
- Problem Based Learning
- Major essay

PG - Engaged and Responsible, Active and Ethical Citizens

Our postgraduates will be ethically aware and capable of confident transformative action in relation to their professional responsibilities and the wider community. They will have a sense of connectedness with others and country and have a sense of mutual obligation. They will be able to appreciate the impact of their professional roles for social justice and inclusion related to

national and global issues

This graduate capability is supported by:

Learning outcomes

- Demonstrate a comprehensive understanding of past, current cyber threats and future trends in high tech crime.
- Analyse the impact of cyber crime on government, businesses, society and individuals.
- Demonstrate knowledge of relevant theories, cross disciplinary approaches (criminology and information security), and the applicability to the study of cyber crime.
- Demonstrate a comprehensive understanding of strategies and steps to investigate digital evidence.

Assessment tasks

- Participation/ engagement
- Critical Review
- Quizzes
- Problem Based Learning
- Major essay