PICT840

Cybercrime

S2 External 2013

Centre for Policing, Intelligence and Counter Terrorism

Contents

General Information

Unit convenor and teaching staff
Other Staff
Vincent Williams
vince.williams@mq.edu.au
Contact via vince.williams@mq.edu.au
Y3A 238
As detailed on the iLearn site

Unit Convenor
Allan Watt
allan.watt@mq.edu.au
Contact via allan.watt@mq.edu.au
Rm 240, Level 2, Building Y3A
By appointment

Credit points
4

Prerequisites
Admission to MPICT or PGDipPICT or PGCertPICT or MPICTMIntSecSt or MIntSecStud or PGDipIntSecStud or PGCertIntSecStud or MCompForens or PGDipCompForens or PGCertCompForens

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 interesting 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, investigation techniques, and counter measures.

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:

Interpret the various aspects of Cybercrime theory and what constitutes criminal and noncriminal offending.
Classify different incidents into the main cybercrime categories.
Identify the perpetrators and recognise the threat level each play in the cybercrime environment.
Synthesis core investigation techniques and devise a comprehensive investigation plan.
Assess relevant counter measures and their legality in performing such acts on both local and international targets.

Assessment Tasks

Name	Weighting	Due
PowerPoint Presentation	20%	25 August 2013
Essay	40%	6 October 2013
Plan	40%	3 November 2013

PowerPoint Presentation

Due: **25 August 2013**
Weighting: **20%**

Review the unit reference material and other suitable sources to create a presentation on various aspects of Cybercrime theory and what constitutes criminal and noncriminal offending and which of the main categories they fall into. Students will be required to complete a PowerPoint Presentation with notes, that if presented would extend to around 10 to 20 minutes (10 slides +/-).

The PowerPoint, must contain Speaker Notes as bullet points with appropriate references within the speakers notes section for each slide.

A detailed marking matrix is available to all enrolled students on the unit iLearn site.

Marking criteria in the marking matrix includes evaluation of topic comprehension, argument,

written expression, referencing, PowerPoint structure and organisation.

On successful completion you will be able to:

- Interpret the various aspects of Cybercrime theory and what constitutes criminal and noncriminal offending.
- Classify different incidents into the main cybercrime categories.

Essay

Due: **6 October 2013**
Weighting: **40%**

The question on whether state nations or even larger organisations who are the victims of a cyber attack should be able to launch a destructive counter attack, raises many issues.

Students need to conduct in-depth research on what the issues are, legally, technically and the risks imposed by conducting such counter attacks. They should then prepare an essay based on their findings. Word length 2000 to 2500 words.

A detailed marking matrix is available to all enrolled students on the unit iLearn site.

Marking criteria in the marking matrix includes evaluation of topic comprehension, argument, written expression, referencing, essay structure and organisation.

On successful completion you will be able to:

- Identify the perpetrators and recognise the threat level each play in the cybercrime environment.
- Assess relevant counter measures and their legality in performing such acts on both local and international targets.

Plan

Due: **3 November 2013**
Weighting: **40%**

It is critical that students understand the various aspects of cybercrime theory. It is equally critical that students further be able implement this into practice. This assessment will test students understanding of the relevant cybercrime theory and demonstrate their understanding when putting it into practice, as demonstrated with the production of a pre-investigation plan and orders.

Word length 3000 words.

A detailed marking matrix is available to all enrolled students on the unit iLearn site.

Marking criteria in the marking matrix includes evaluation of topic comprehension, written

expression, referencing, plan and orders structure and organisation and workability.

On successful completion you will be able to:

- Interpret the various aspects of Cybercrime theory and what constitutes criminal and noncriminal offending.
- Classify different incidents into the main cybercrime categories.
- Identify the perpetrators and recognise the threat level each play in the cybercrime environment.
- Synthesis core investigation techniques and devise a comprehensive investigation plan.

Delivery and Resources

UNIT REQUIREMENTS AND EXPECTATIONS

You should spend an average of at least 12 hours per week on this unit. This includes listening to pre-recorded lectures prior to seminar discussions and reading weekly required readings detailed in iLearn.

Internal students are expected to attend all seminar sessions and external students are expected to contribute to on-line discussions.

REQUIRED READINGS

The citations for all the required readings for this unit are available to enrolled students through the unit iLearn site, the CD reading list and at Macquarie University's Library EReserve site. Electronic copies of required readings may be accessed at the EReserve site.

RECOMMENDED READINGS

Recommended readings will be posted to the unit iLearn site as Session 2 progresses.

While there is no prescribed textbook for this unit students may consider obtaining a copy of

• Computer Forensics, Electronic Discovery and Electronic Evidence Stanfield, A; LexisNexis Butterworths, Sydney, 2009

TECHNOLOGY USED AND REQUIRED

Personal PC and internet access are essential for this unit. Basic computer skills and skills in word processing are also a requirement.

The unit can only be accessed by enrolled students online through http://ilearn.mq.edu.au

SUBMITTING ASSESSMENT TASKS

All assessment tasks are to be submitted, marked and returned electronically. This will only happen through the unit iLearn site.

Assessment tasks must be submitted either as a PDF or MS word document by the due date.

All assessment tasks will be subject to a 'TurnitIn' review as an automatic part of the submission process.

Assessment tasks must be submitted with a plagiarism declaration. This may be as part of the task submission process through grademark or through completion of a coversheet. The coversheet can be downloaded at:

www.arts.mq.edu.au/current_students/postgraduate_coursework.

The granting of extensions of up to one week are at the discretion of the unit convenor. Any requests for extensions must be made in writing before the due date for the submission of the assessment task. Extensions beyond one week are subject to special consideration. The policy for this is detailed under Policy and Procedures.

LATE SUBMISSION OF ASSESSMENT TASKS

There is a penalty for the late submission of assessment tasks. If an assignment is submitted late it will initially be marked as if it had been submitted on time.

However, 5%of the weighting allocated for the assignment will then be deducted from the mark the student initially achieves in the assessment task for each day it is late. For example if the assessment task's weighting is 20, 1.00 mark per day will be deducted from the initial mark given per day it is late ie a task initially given 15/20 but which is submitted four days late will lose 4 x 1.00 marks. That means 15/20-4 marks=11/20. It is this second mark which will be recorded in gradebook.

The same principle applies if a student seeks and is granted an extension and the assessment task is submitted later than the amended submission date.

Unit Schedule

Week 1	**Introduction and Unit Overview** · Introductions · Course Organisation · Learning Approach · Assessment · Expectations · Cyber Crime defined
Week 2	**Cyber Crime Cases**
Week 3	**Cyber Criminals**
Week 4	**Cyber Law I**
Week 5	**Cyber Law II**
Week 6	**Counter Measures**
Week 7	**Pre Investigation Planning/Management**
Week 8	**Scene Attendance**
Week 9	**Digital Forensics I**
Week 10	**Digital Forensics II & Mobile Forensics**
Week 11	**e.discovery**
Week 12	**Cyber Space Investigations**
Week 13	**Future trends**

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://www.mq.edu.au/policy/docs/academic_honesty/policy.html

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

Grading Policy http://www.mq.edu.au/policy/docs/grading/policy.html

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

Grievance Management Policy http://mq.edu.au/policy/docs/grievance_management/policy.html

Special Consideration Policy http://www.mq.edu.au/policy/docs/special_consideration/policy.html

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

Student Support

Macquarie University provides a range of Academic Student Support Services. Details of these services can be accessed at: http://students.mq.edu.au/support/

UniWISE provides:

- Online learning resources and academic skills workshops http://www.students.mq.edu.au/support/learning_skills/
- Personal assistance with your learning & study related questions.
- The Learning Help Desk is located in the Library foyer (level 2).
- Online and on-campus orientation events run by Mentors@Macquarie.

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

Details of these services can be accessed at http://www.student.mq.edu.au/ses/.

IT Help

If you wish to receive IT help, we would be glad to assist you at http://informatics.mq.edu.au/help/.

When using the university's IT, you must adhere to the Acceptable Use Policy. The policy applies to all who connect to the MQ network including students and it outlines what can be done.

Graduate Capabilities

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

- Interpret the various aspects of Cybercrime theory and what constitutes criminal and noncriminal offending.

- Classify different incidents into the main cybercrime categories.
- Identify the perpetrators and recognise the threat level each play in the cybercrime environment.
- Synthesis core investigation techniques and devise a comprehensive investigation plan.
- Assess relevant counter measures and their legality in performing such acts on both local and international targets.

Assessment tasks

- PowerPoint Presentation
- Essay
- Plan

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

- Interpret the various aspects of Cybercrime theory and what constitutes criminal and noncriminal offending.
- Classify different incidents into the main cybercrime categories.
- Identify the perpetrators and recognise the threat level each play in the cybercrime environment.
- Synthesis core investigation techniques and devise a comprehensive investigation plan.
- Assess relevant counter measures and their legality in performing such acts on both local and international targets.

Assessment tasks

- PowerPoint Presentation
- Essay
- Plan

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

- Interpret the various aspects of Cybercrime theory and what constitutes criminal and noncriminal offending.
- Classify different incidents into the main cybercrime categories.
- Identify the perpetrators and recognise the threat level each play in the cybercrime environment.
- Synthesis core investigation techniques and devise a comprehensive investigation plan.
- Assess relevant counter measures and their legality in performing such acts on both local and international targets.

Assessment tasks

- PowerPoint Presentation
- Essay
- Plan

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

- Interpret the various aspects of Cybercrime theory and what constitutes criminal and noncriminal offending.
- Classify different incidents into the main cybercrime categories.
- Identify the perpetrators and recognise the threat level each play in the cybercrime environment.
- Synthesis core investigation techniques and devise a comprehensive investigation plan.
- Assess relevant counter measures and their legality in performing such acts on both local and international targets.

Assessment tasks

- PowerPoint Presentation
- Essay

- Plan

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 outcome

- Synthesis core investigation techniques and devise a comprehensive investigation plan.

Assessment task

- Plan

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

- Interpret the various aspects of Cybercrime theory and what constitutes criminal and noncriminal offending.
- Classify different incidents into the main cybercrime categories.
- Identify the perpetrators and recognise the threat level each play in the cybercrime environment.
- Synthesis core investigation techniques and devise a comprehensive investigation plan.
- Assess relevant counter measures and their legality in performing such acts on both local and international targets.

Assessment tasks

- PowerPoint Presentation
- Essay
- Plan