PICT848

Cyber Security

S1 Evening 2013

Centre for Policing, Intelligence and Counter Terrorism

Contents

General Information

Unit convenor and teaching staff
Unit Convenor
Milton Baar
milton.baar@mq.edu.au
Contact via milton.baar@mq.edu.au

Credit points
4

Prerequisites
Admission to MPICT or PGDipPICT or PGCertPICT or MPICTMIntSecSt or MIntSecStud or PGDipIntSecStud or PGCertIntSecStud.

Corequisites

Co-badged status

Unit description
This unit is an introduction to cyber security threats, technologies and management practices within the public and private sectors. The threats faced in the cyber world in many ways mirror those in the physical world. Despite that they also differ in nature as they are neither inhibited by geography nor political borders. This unit will consider these threats in that context. The unit will also provide a sound understanding of the governing principles behind cyber security, the theory and practice behind technology risks and countermeasures and the role that security management plays in the wider picture of forensics analysis, policing, intelligence and counter terrorism.

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:

To gain a fundamental understanding of Cybersecurity technologies that underpin the operational environment

To gain a greater awareness of the procedures and practices involved in managing Cybersecurity risks

To gain a greater awareness of the procedures and practices involved in

countermeasures to cybersecurity threats

Develop analytical skills and demonstrate the ability to communicate information

Develop a solid foundation for further study into the field of cybercrime and cybersecurity

Assessment Tasks

Name	Weighting	Due
Literature review	10%	Weekly
Weekly discussion	10%	Weekly
Minor assignment	30%	24/3/2013
Major assignment	50%	9/6/2013

Literature review

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

Each week students are to read the weekly essential reading. For this assessment task, students must select one of the texts and provide an approximately 250-word critique. Your critique should summarise the key concepts underpinning the reading, describe how the reading is situated in the context of the other issues being addressed in this session, and also provide an evaluation of the reading. Students are to post their critique to the Reading Critique Discussion section on iLearn for the week and are expected to provide responses (questions, comments or counterpoints) to the contributions of others.

On successful completion you will be able to:

- To gain a fundamental understanding of Cybersecurity technologies that underpin the operational environment
- To gain a greater awareness of the procedures and practices involved in managing Cybersecurity risks
- To gain a greater awareness of the procedures and practices involved in countermeasures to cybersecurity threats
- Develop analytical skills and demonstrate the ability to communicate information
- Develop a solid foundation for further study into the field of cybercrime and cybersecurity

Weekly discussion

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

The weekly post lecture discussions are based on the content of the lectures. They are

designed to promote critical reflection upon the concepts being addressed. Students are to consider them carefully and then engage in online discussion with peers. Thoughts are to be posted to the discussion board, and responses to other people's postings are to be provided.

On successful completion you will be able to:

- To gain a fundamental understanding of Cybersecurity technologies that underpin the operational environment
- To gain a greater awareness of the procedures and practices involved in managing Cybersecurity risks
- To gain a greater awareness of the procedures and practices involved in countermeasures to cybersecurity threats
- Develop analytical skills and demonstrate the ability to communicate information
- Develop a solid foundation for further study into the field of cybercrime and cybersecurity

Minor assignment

Due: **24/3/2013**
Weighting: **30%**

Cyber security research and responses are spread across of broad range of topic domains. Using published research papers available through internet searches, identify the most significant domains of published research and analyse commercial responses to the research.

The assessment rubric is on iLearn.

On successful completion you will be able to:

- To gain a fundamental understanding of Cybersecurity technologies that underpin the operational environment
- To gain a greater awareness of the procedures and practices involved in managing Cybersecurity risks
- To gain a greater awareness of the procedures and practices involved in countermeasures to cybersecurity threats
- Develop analytical skills and demonstrate the ability to communicate information

Major assignment

Due: **9/6/2013**
Weighting: **50%**

Compare the Australian Government approach to cybersecurity with the Council of Europe's approach. Analyse and comment on how the Government approaches help or hinder the private sector in their approach to managing cybersecurity.

The assessment rubric is on iLearn.

On successful completion you will be able to:

- To gain a fundamental understanding of Cybersecurity technologies that underpin the operational environment
- To gain a greater awareness of the procedures and practices involved in managing Cybersecurity risks
- To gain a greater awareness of the procedures and practices involved in countermeasures to cybersecurity threats
- Develop analytical skills and demonstrate the ability to communicate information

Delivery and Resources

This unit is delivered online and on-campus. Online units can be accessed at: http://ilearn.mq.edu.au

PC and Internet access are required. Basic computer skills (e.g., internet browsing) and skills in word processing are also a requirement.

Please consult teaching staff for any further, more specific requirements.

If an assignment is submitted late, **5%** of the available mark will be deducted for each day the paper is late. For example, if the paper is worth 20 marks, 1.00 mark per day will be deducted from the mark given (ie. A student given 15/20 who submitted 4 days late will lose 4 x 1.00 marks: 15/20 – 4 marks = 11/20) The same principle applies if an extension is granted and the assignment is submitted later than the amended date.

Unit Schedule

Unit schedule may be found on iLearn

Learning and Teaching Activities

Weekly audio presentation

Each week, prior to attending class if on-campus or prior to interacting on iLearn, students must listen to the audio lecture and read the notes and critically analyse the contents.

Weekly discussion

Each week, students must discuss and interact with each other based on their critical review and analysis of the weekly material. If on-campus, the interaction will take place in the weekly classes and on iLearn, if off-campus, the interaction is through iLearn alone.

Weekly reading

Each week, prior to attending class if on-campus or prior to interacting on iLearn, students must read the weekly reference material and critically analyse the contents.

Assessment tasks

Assessment tasks are used to reinforce learning outcomes.

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

- To gain a fundamental understanding of Cybersecurity technologies that underpin the operational environment
- To gain a greater awareness of the procedures and practices involved in managing Cybersecurity risks
- To gain a greater awareness of the procedures and practices involved in countermeasures to cybersecurity threats

Assessment tasks

- Literature review
- Weekly discussion

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

- Develop analytical skills and demonstrate the ability to communicate information
- Develop a solid foundation for further study into the field of cybercrime and cybersecurity

Assessment tasks

- Literature review
- Weekly discussion

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 outcome

- Develop analytical skills and demonstrate the ability to communicate information

Assessment tasks

- Minor assignment
- Major assignment

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

- Develop analytical skills and demonstrate the ability to communicate information
- Develop a solid foundation for further study into the field of cybercrime and cybersecurity

Assessment tasks

- Literature review
- Weekly discussion
- Minor assignment
- Major assignment

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

- Develop a solid foundation for further study into the field of cybercrime and cybersecurity

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

- To gain a greater awareness of the procedures and practices involved in countermeasures to cybersecurity threats
- Develop a solid foundation for further study into the field of cybercrime and cybersecurity

Assessment tasks

- Literature review
- Weekly discussion
- Minor assignment
- Major assignment