PICT706

Understanding Cyber Security

S1 External 2016

Dept of Policing, Intelligence & Counter-Terrorism

Contents

General Information	2
Learning Outcomes	2
Assessment Tasks	3
Delivery and Resources	7
Unit Schedule	9
Policies and Procedures	9
Graduate Capabilities	11
Changes since First Published	14

General Information

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

Angela Irwin
angela.irwin@mq.edu.au

Credit points
4

Prerequisites
Admission to MRes

Corequisites

Co-badged status
PICT848

Unit description
This unit exposes students to significant issues relating to security studies in one of five identified areas. These five areas - policing, intelligence, counter terrorism, cybersecurity and international security - are central to an understanding of security within a rapidly changing global context. The unit challenges students to test the limits of research in a selected area of study and identify effective research methodologies relevant to this area.

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:

Demonstrate a comprehensive understanding of cyber security threats, technologies and management practices within public and private sectors.
Critique and evaluate threats faced in the cyber world and contrast them against those in the physical world.
Evaluate the significance and relevance 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 cyber security.

Demonstrate a comprehensive awareness of the procedures and practices involved in managing cyber security risks and threats and apply these to a real world situation, through the establishment of a cyber security risk assessment exercise.

Assessment Tasks

Name	Weighting	Due
Participation/Engagement	25%	Weekly
Research essay	25%	See unit iLearn site
Cyber security risk assessment	50%	See unit iLearn site

Participation/Engagement

Due: **Weekly**
Weighting: **25%**

Internal students

Your participation in class should demonstrate that you have read, understood and reflected on course material and weekly readings. You should bring in related thoughts and material, readings or questions that occur to you throughout the discussion.

You are required to complete the core readings for each module, reflect upon the readings and to then share your reflections on the readings with course colleagues during the on-campus sessions.

Your discussions should advance the group's negotiation 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, personal experience or readings;
- commenting on or expanding another student's statement;
- posing a substantive question aimed at furthering the group's understanding. of the topic.

A variety of different activities will occur each week and students should be prepared to fully participate in these activities. Students are also to actively engage with other students in class and challenge their input.

This task is to assess your comprehension of the weekly material and that you are engaging with the Unit.

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

1. Your participation in the discussions (40%)
2. The essence of your contributions (60%)

In assessing your contributions, the following categories will be used:

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

Attendance and participation in class discussions is worth 10% of the engagement and participation score.

On some weeks, internal students will be required to complete lab exercises. These lab exercises will involve the use of common cyber security tools. Students must complete lab sheets each week to show the results of their lab exercises and answers to questions posed. Students will be required to submit their lab exercise sheets for marking after the final lab session (week to be confirmed).

The lab exercise component of the unit is worth 15% of the engagement and participation score.

External students

Your postings to the online discussion forums should demonstrate that you have read, understood and reflected on course material and weekly readings. You should bring in related thoughts and material, readings or questions that occur to you throughout the discussion. You are required to complete the core readings for each module, reflect upon the readings and share your reflections on the readings with course colleagues through online discussion forum questions. One question will be posted to the discussion forum each week. Responses to each question should be a minimum of 100 words in length.

Forum discussion question postings should advance the group's negotiation 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, personal experience or readings;
- commenting on or expanding another student’s statement;
- posting a substantive question aimed at furthering the group’s understanding of the topic.

If citing course readings, in-text references are sufficient. For additional references (if applicable), please provide a bibliographic reference at the end of your post. 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 they are entered later than this, they will not be counted.

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

1. Your participation in the discussions (40%)

2. The essence of your contributions (60%)

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.

External students will be required to complete three quizzes during the unit (weeks to be confirmed). The quizzes will be based around the readings or course materials for specified weeks.

Each quiz will be worth 5% of the engagement and participation score (i.e. 15% in total).

On successful completion you will be able to:

- Demonstrate a comprehensive understanding of cyber security threats, technologies and management practices within public and private sectors.
- Critique and evaluate threats faced in the cyber world and contrast them against those in the physical world.
- Evaluate the significance and relevance 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 cyber security.
- Demonstrate a comprehensive awareness of the procedures and practices involved in managing cyber security risks and threats and apply these to a real world situation, through the establishment of a cyber security risk assessment exercise.

Research essay

Due: **See unit iLearn site**
Weighting: **25%**

CIA is the underlying concept of providing uninterrupted, continuous and reliable access to information resources. Critically examine the CIA concept identifying the strengths and weaknesses of it and compare and contrast it against other similar models. 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:

- Demonstrate a comprehensive understanding of cyber security threats, technologies and management practices within public and private sectors.
- Critique and evaluate threats faced in the cyber world and contrast them against those in the physical world.
- Evaluate the significance and relevance 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 cyber security.

Cyber security risk assessment

Due: **See unit iLearn site**
Weighting: **50%**

Effective cyber security risk management is much more than a technology solution, it must be integrated into an organisation's day-to-day operations. A company must be prepared to respond to the inevitable cyber incident, restore normal operations and ensure that company assets and the company's reputation are protected. In this assessment, students must perform a risk analysis of a scenario organisation's cyber risk, identify threats and vulnerabilities of information assets, forecast the consequences of a successful attack and recommend how each threat should be treated.

The risk assessment must be able to cater for accidental or deliberate hardware, software and network failures.

The 3,500 word risk assessment allows students to explore the application of cyber security principals to a real world organisation. A scenario will be provided to students later in the session. A detailed marking matrix is available to all enrolled students on the unit iLearn site. Marking criteria includes evaluation of understanding of risk assessment concepts, written expression, referencing, structure and layout and workability of the risk assessment provided.

On successful completion you will be able to:

- Demonstrate a comprehensive understanding of cyber security threats, technologies and management practices within public and private sectors.
- Critique and evaluate threats faced in the cyber world and contrast them against those in the physical world.
- Evaluate the significance and relevance 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 cyber security.
- Demonstrate a comprehensive awareness of the procedures and practices involved in managing cyber security risks and threats and apply these to a real world situation, through the establishment of a cyber security risk assessment exercise.

Delivery and Resources

UNIT REQUIREMENTS AND EXPECTATIONS

- You should spend an average of at least 9 hours per week on this unit. This includes completing weekly activities and readings detailed in iLearn.
- Internal students are expected to attend all seminars and external students are expected to contribute to weekly on-line discussions.
- Students are required to 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 EReserve site. Electronic copies of required readings may be accessed at the EReserve site.

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.
- 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.
- For technical support go to: http://mq.edu.au/about_us/offices_and_units/informatics/help
- For student quick guides on the use of iLearn go to: http://mq.edu.au/iLearn/student_info/guides.htm

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.
- Assessment tasks will be subject to a 'TurnitIn' review as an automatic part of the submission process.
- The granting of extensions of up to one week are at the discretion of the unit convener. 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 the university's Disruptions Policy (http://www.mq.edu.au/policy/docs/disruption_studies/policy.html#purpose).

LATE SUBMISSION OF ASSESSMENT TASKS

- If an assignment is submitted late, 5% of the available mark will be deducted for each day the assessment is late (including weekends)
- 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 do not include references, 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.
- The application of this penalty is at the discretion of the unit 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://mq.edu.au/policy/docs/gradeappeal/policy.html). This process involves all assignments submitted for that unit being reassessed. However, in exceptional cases students may request that a single piece of work is reassessed. The Department process for the reassessment of assignments for marking during the semester is as follows:
- You must consult with the unit convenor - A reassessment will only be granted if you have sought and received feedback about your performance on the assessment from the convenor.
- Apply to PICT's Director of Learning and Teaching (or delegated authority) for a reassessment - no more than 7 days after the unit convenor or class tutor has returned the assessment to you. You must make a sound academic case referring to the marking rubric, which demonstrates that you have consulted the unit convenor and as a result of this there is evidence that either the marking criteria were not provided, or there is insufficient feedback to justify the mark given.
- If appropriate, the Head of Department (or delegated authority) will organise the

reassessment of work.

- The mark determined after reassessment will be the final mark in that assessment task, and this mark can be lower than the original.

Unit Schedule

Week 1 - Introduction to cyber security

Week 2 - Access control

Week 3 - Telecommunications and network security

Week 4 - Information security and risk management

Week 5 - Application security

Week 6 - Cryptography

Week 7 - Security architecture and design

Week 8 - Operations security

Week 9 - Business continuity and disaster recovery planning

Week 10 - Legal, regulations, compliance and investigations

Week 11 - Physical (environmental) security

Week 12 - Training, behaviours and social engineering

Week 13 - Unit review

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

New Assessment Policy in effect from Session 2 2016 http://mq.edu.au/policy/docs/assessment/policy_2016.html. For more information visit http://students.mq.edu.au/events/2016/07/19/new_assessment_policy_in_place_from_session_2/

Assessment Policy prior to Session 2 2016 http://mq.edu.au/policy/docs/assessment/policy.html

Grading Policy prior to Session 2 2016 http://mq.edu.au/policy/docs/grading/policy.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 http://www.mq.edu.au/policy/docs/disruption_studies/policy.html *The Disruption to Studies Policy is effective from March 3 2014 and replaces the Special Consideration Policy.*

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

- Demonstrate a comprehensive understanding of cyber security threats, technologies and management practices within public and private sectors.
- Critique and evaluate threats faced in the cyber world and contrast them against those in the physical world.
- Evaluate the significance and relevance 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 cyber security.
- Demonstrate a comprehensive awareness of the procedures and practices involved in managing cyber security risks and threats and apply these to a real world situation, through the establishment of a cyber security risk assessment exercise.

Assessment tasks

- Participation/Engagement
- Research essay
- Cyber security risk assessment

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

- Demonstrate a comprehensive understanding of cyber security threats, technologies and management practices within public and private sectors.
- Critique and evaluate threats faced in the cyber world and contrast them against those in the physical world.
- Evaluate the significance and relevance 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 cyber security.
- Demonstrate a comprehensive awareness of the procedures and practices involved in managing cyber security risks and threats and apply these to a real world situation, through the establishment of a cyber security risk assessment exercise.

Assessment tasks

- Participation/Engagement
- Research essay
- Cyber security risk assessment

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

- Demonstrate a comprehensive understanding of cyber security threats, technologies and management practices within public and private sectors.
- Critique and evaluate threats faced in the cyber world and contrast them against those in the physical world.
- Evaluate the significance and relevance 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 cyber security.
- Demonstrate a comprehensive awareness of the procedures and practices involved in managing cyber security risks and threats and apply these to a real world situation, through the establishment of a cyber security risk assessment exercise.

Assessment tasks

- Participation/Engagement
- Research essay
- Cyber security risk assessment

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

- Demonstrate a comprehensive understanding of cyber security threats, technologies and management practices within public and private sectors.
- Critique and evaluate threats faced in the cyber world and contrast them against those in the physical world.
- Evaluate the significance and relevance 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 cyber security.
- Demonstrate a comprehensive awareness of the procedures and practices involved in managing cyber security risks and threats and apply these to a real world situation, through the establishment of a cyber security risk assessment exercise.

Assessment tasks

- Participation/Engagement
- Research essay
- Cyber security risk assessment

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

- Demonstrate a comprehensive understanding of cyber security threats, technologies and management practices within public and private sectors.
- Critique and evaluate threats faced in the cyber world and contrast them against those in the physical world.
- Evaluate the significance and relevance 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 cyber security.
- Demonstrate a comprehensive awareness of the procedures and practices involved in managing cyber security risks and threats and apply these to a real world situation,

through the establishment of a cyber security risk assessment exercise.

Assessment tasks

- Participation/Engagement
- Research essay
- Cyber security risk assessment

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 cyber security threats, technologies and management practices within public and private sectors.
- Critique and evaluate threats faced in the cyber world and contrast them against those in the physical world.
- Evaluate the significance and relevance 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 cyber security.
- Demonstrate a comprehensive awareness of the procedures and practices involved in managing cyber security risks and threats and apply these to a real world situation, through the establishment of a cyber security risk assessment exercise.

Assessment tasks

- Participation/Engagement
- Cyber security risk assessment

Changes since First Published

Date	Description
11/01/2016	For approval by HoD.