PICT848

Cyber Security

S1 Evening 2017

Department of Security Studies and Criminology

Contents

General Information

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

Credit points
4

Prerequisites
Admission to MPICT or MCPICT or PGDipPICT or GradDipPICT or GradDipCPICT or PGCertPICT or GradCertPICT or GradCertCPICT or MPICTMIntSecSt or MCPICTMIntSecSt or MIntSecStud or GradDipIntSecStud or GradCertIntell or MInfoTech or MCRIM

Corequisites

Co-badged status
PICT706

Unit description
In today's world, organisations must be able to protect and defend against threats in cyberspace. This unit provides a solid understanding of the theory and practice used to manage information security on computer systems and networks. Students will be exposed to multiple cyber security technologies, processes and procedures, learn how to analyse threats, vulnerabilities and risks present in these environments, and develop appropriate strategies to mitigate potential cyber security problems. Topics include: an overview of computer and communications security, risk assessment, human factors, identification and authentication, access controls, malicious software, software security and legal and ethical issues. Students will have the opportunity to use tools and software commonly used to attack/protect networks.

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	Hurdle	Due
Engagement/participation	25%	No	Weekly
Research essay	25%	No	See unit iLearn site
Cyber security risk assessment	50%	No	See unit iLearn site

Engagement/participation

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 research 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.

Students who do not fully participate in at least 8 discussion forums will receive a marks of zero for this component of participation. External students will also 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 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
- Conforming to the Grade Appeal Policy, individual works are not subject to regrading.

STAFF AVAILABILITY

- Department staff will endeavor 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.

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

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

- 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

- Engagement/participation
- 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

- Engagement/participation
- 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

- Engagement/participation
- 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

- Engagement/participation
- 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

- Engagement/participation
- 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

- Critique and evaluate threats faced in the cyber world and contrast them against those in the physical world.
- 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

- Engagement/participation
- Cyber security risk assessment