PICT8048

Applied Cyber Security

Session 1, Fully online/virtual 2021

Department of Security Studies and Criminology

Contents

Notice

As part of Phase 3 of our return to campus plan, most units will now run tutorials, seminars and other small group activities on campus, and most will keep an online version available to those students unable to return or those who choose to continue their studies online.

To check the availability of face-to-face activities for your unit, please go to timetable viewer. To check detailed information on unit assessments visit your unit's iLearn space or consult your unit convenor.

General Information

Unit convenor and teaching staff
Ed Moore
ed.moore@mq.edu.au

Credit points
10

Prerequisites
Admission to MPICT or MCPICT or GradDipPICT or GradDipCPICT or PGCertPICT or GradCertPICT or GradCertCPICT or MPICTMIntSecSt or MCPICTMIntSecSt or MIntSecStud or GradDipIntSecStud or GradCertIntell or MInfoTech or MCyberSec or MSecStrategicStudMCyberSec or MIntellMCyberSec or MCyberSecMCTerrorism or MCyberSecMCrim or Master of Cyber Security Analysis or admission to BSecStudMCyberSecAnalysis

Corequisites

Co-badged status

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 and policies 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 in order to develop workplace skills.

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:

ULO1: Demonstrate a comprehensive understanding of cyber security threats,

technologies and management practices within public and private sectors.

ULO2: 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

ULO3: Critique and evaluate threats faced in the cyber world and contrast them against those in the physical world.

ULO4: 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
Tutorial Exercises	10%	No	Ongoing
Weekly Quizzes	20%	No	Weeks 1-12
Major Essay	50%	No	Week 8
Major Quiz	20%	No	Week 13

Tutorial Exercises

Assessment Type [1]: Participatory task
Indicative Time on Task [2]: 13 hours
Due: **Ongoing**
Weighting: **10%**

Participation in tutorial based exercises (for internal students) and forum based discussion (for external students).

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.
- 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

Weekly Quizzes

Assessment Type [1]: Quiz/Test
Indicative Time on Task [2]: 20 hours
Due: **Weeks 1-12**
Weighting: **20%**

Online weekly quizzes based on the content from the previous week to be completed by all students.

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.
- 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

Major Essay

Assessment Type [1]: Essay
Indicative Time on Task [2]: 40 hours
Due: **Week 8**
Weighting: **50%**

Essay task on a current cyber security issue.

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.
- 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
- 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

Major Quiz

Assessment Type [1]: Quiz/Test
Indicative Time on Task [2]: 20 hours

Due: **Week 13**
Weighting: **20%**

Major quiz to test knowledge of all topics of the course

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.
- 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

---

[1] If you need help with your assignment, please contact:

- the academic teaching staff in your unit for guidance in understanding or completing this type of assessment
- the Writing Centre for academic skills support.

[2] Indicative time-on-task is an estimate of the time required for completion of the assessment task and is subject to individual variation

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 Special Consideration Policy. Extensions will not be granted by unit conveners or tutors, but must be lodged through Special Consideration: https://students.mq.edu.au/study/my-study-program/special-consideration

LATE SUBMISSION OF ASSESSMENT TASKS

- Unless a Special Consideration request has been submitted and approved, (a) **a penalty for lateness will apply** – two (2) marks out of 100 will be deducted per day for assignments submitted after the due date – and (b) **no assignment will be accepted seven (7) days (incl. weekends) after the original submission deadline**. No late submissions will be accepted for timed assessments – e.g. quizzes, online tests.

Unit Schedule

Week 1	Security Governance
Week 2	Personnel Security, Risk Management & Business Continuity
Week 3	Laws, Regulations and Compliance | Protecting assets
Week 4	Cryptography
Week 5	Security Models | Security Vulnerabilities

Week 6	Physical Security
Week 7	Secure Networks
Week 8	Identity, Authentication | Controlling Access
Week 9	Security Assessment and Testing | Security Operations
Week 10	Preventing and Responding to incidents | Disaster Recovery
Week 11	Investigations and Ethics
Week 12	Secure Software | Malware
Week 13	Review

Policies and Procedures

Macquarie University policies and procedures are accessible from Policy Central (https://policies.mq.edu.au). Students should be aware of the following policies in particular with regard to Learning and Teaching:

- Academic Appeals Policy
- Academic Integrity Policy
- Academic Progression Policy
- Assessment Policy
- Fitness to Practice Procedure
- Grade Appeal Policy
- Complaint Management Procedure for Students and Members of the Public
- Special Consideration Policy

Students seeking more policy resources can visit Student Policies (https://students.mq.edu.au/support/study/policies). It is your one-stop-shop for the key policies you need to know about throughout your undergraduate student journey.

To find other policies relating to Teaching and Learning, visit Policy Central (https://policies.mq.edu.au) and use the search tool.

Student Code of Conduct

Macquarie University students have a responsibility to be familiar with the Student Code of Conduct: https://students.mq.edu.au/admin/other-resources/student-conduct

Results

Results published on platform other than eStudent, (eg. iLearn, Coursera etc.) 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 or if you are a Global MBA student contact globalmba.support@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 help you improve your marks and take control of your study.

- Getting help with your assignment
- Workshops
- StudyWise
- Academic Integrity Module

The Library provides online and face to face support to help you find and use relevant information resources.

- Subject and Research Guides
- Ask a Librarian

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

If you are a Global MBA student contact globalmba.support@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.

Changes since First Published

Date	Description
03/02/2021	Updated late penalty statement.