PICT3011
Cyber Security in Practice
Session 2, Fully online/virtual 2021

Department of Security Studies and Criminology

Contents

General Information 2
Learning Outcomes 2
Assessment Tasks 3
Delivery and Resources 5
Policies and Procedures 7
Changes since First Published 9

Disclaimer
Macquarie University has taken all reasonable measures to ensure the information in this publication is accurate and up-to-date. However, the information may change or become out-dated as a result of change in University policies, procedures or rules. The University reserves the right to make changes to any information in this publication without notice. Users of this publication are advised to check the website version of this publication [or the relevant faculty or department] before acting on any information in this publication.

Notice
Some on-campus classes have moved online for the first two weeks of Session, before returning to campus in Week 3. If you are studying a unit outside of the primary Session 2 timetable, please contact your teaching staff team for further details.

Some classes/teaching activities cannot be moved online and must be taught on campus. To find out if you are enrolled in one of these classes/teaching activities, you can check to see if your unit is on the list of units with mandatory on-campus classes/teaching activities.

Your Unit Convenor will provide more information via an iLearn announcement when your iLearn unit becomes available.

https://unitguides.mq.edu.au/unit_offerings/134055/unit_guide/print
General Information

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

Credit points
10

Prerequisites
50cp at 2000 level or above

Corequisites

Co-badged status

Unit description
Computer systems and networks, and the applications that they support, are essential to information flows, economic transactions and critical infrastructure in the twenty-first century. This unit will present an overview of modern cyber security with reference to both public and private sector organisations. The unit will look at the motives and perpetrators of cybercrime. It will explore how individuals and organisations face specific threats from their use of technology and identify challenges in maintaining cyber and information security. It further examines the protective security measures required to protect physical and digital access to information through people, infrastructure and computer systems.

Important Academic Dates
Information about important academic dates including deadlines for withdrawing from units are available at https://students.mq.edu.au/important-dates

Learning Outcomes
On successful completion of this unit, you will be able to:

ULE1: Integrate and analyse relevant theoretical and case-based literature to present a sustained, coherent and logical consideration to cybercrime and cyber security
ULE2: Demonstrate a comprehensive understanding of the key procedures and practices relevant to the management of cyber security risks and countermeasures.
ULE3: Demonstrate a comprehensive understanding of threats to computer networks and physical infrastructure.
ULE4: Critique and evaluate key security vulnerabilities of data storage infrastructure.
ULO5: Apply advanced cyber hygiene practices to improve both personal and professional security

## Assessment Tasks

<table>
<thead>
<tr>
<th>Name</th>
<th>Weighting</th>
<th>Hurdle</th>
<th>Due</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tutorial Participation</td>
<td>10%</td>
<td>No</td>
<td>Ongoing</td>
</tr>
<tr>
<td>Weekly Quizzes</td>
<td>20%</td>
<td>No</td>
<td>Weeks 2 - 13</td>
</tr>
<tr>
<td>Seminal Article Critique</td>
<td>20%</td>
<td>No</td>
<td>Week 7</td>
</tr>
<tr>
<td>Research Essay</td>
<td>50%</td>
<td>No</td>
<td>Week 12</td>
</tr>
</tbody>
</table>

### Tutorial Participation

**Assessment Type**: Participatory task

**Indicative Time on Task**: 13 hours

**Due**: Ongoing

**Weighting**: 10%

Student engagement within tutorial exercises (or weekly forums for external students).

On successful completion you will be able to:

- Demonstrate a comprehensive understanding of the key procedures and practices relevant to the management of cyber security risks and countermeasures.
- Demonstrate a comprehensive understanding of threats to computer networks and physical infrastructure.
- Critique and evaluate key security vulnerabilities of data storage infrastructure.
- Apply advanced cyber hygiene practices to improve both personal and professional security.

### Weekly Quizzes

**Assessment Type**: Quiz/Test

**Indicative Time on Task**: 20 hours

**Due**: Weeks 2 - 13

**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 the key procedures and practices relevant to the management of cyber security risks and countermeasures.

• Demonstrate a comprehensive understanding of threats to computer networks and physical infrastructure.

• Critique and evaluate key security vulnerabilities of data storage infrastructure.

• Apply advanced cyber hygiene practices to improve both personal and professional security

Seminal Article Critique

Assessment Type 1: Essay
Indicative Time on Task 2: 20 hours
Due: Week 7
Weighting: 20%

Seminal article critique based on an article of student's choice relevant to a topic from the course to be completed by all students.

On successful completion you will be able to:

• Integrate and analyse relevant theoretical and case-based literature to present a sustained, coherent and logical consideration to cybercrime and cyber security

• Demonstrate a comprehensive understanding of the key procedures and practices relevant to the management of cyber security risks and countermeasures.

• Critique and evaluate key security vulnerabilities of data storage infrastructure.

• Apply advanced cyber hygiene practices to improve both personal and professional security

Research Essay

Assessment Type 1: Essay
Indicative Time on Task 2: 40 hours
Due: Week 12
Weighting: 50%
Research essay to be completed by all students on the given question.

On successful completion you will be able to:

• Integrate and analyse relevant theoretical and case-based literature to present a sustained, coherent and logical consideration to cybercrime and cyber security
• Demonstrate a comprehensive understanding of the key procedures and practices relevant to the management of cyber security risks and countermeasures.
• Demonstrate a comprehensive understanding of threats to computer networks and physical infrastructure.
• Critique and evaluate key security vulnerabilities of data storage infrastructure.
• Apply advanced cyber hygiene practices to improve both personal and professional security

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 Learning Skills Unit 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 – 10 marks out of 100 credit will be deducted per day for assignments submitted after the due date – and (b) no assignment will be accepted seven days (incl. weekends) after the original submission deadline. No late submissions will be accepted for timed assessments - e.g. quizzes, online tests.

WORD LIMITS FOR ASSESSMENT TASKS

• Stated word limits include footnotes and footnoted references, but not bibliography, or
Policies and Procedures

Macquarie University policies and procedures are accessible from Policy Central (https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policy-central). 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

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
- In accordance with the Grade Appeal Policy, individual works are not subject to regrading.

STAFF AVAILABILITY

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

If you would like to see all the policies relevant to Learning and Teaching visit Policy Central (https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/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/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 Enquiry Service
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

Equity 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.

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

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/07/2021</td>
<td></td>
</tr>
</tbody>
</table>