



COMP1300

Introduction to Cyber Security

Session 1, Online-scheduled-weekday 2022

School of Computing

Contents

<u>General Information</u>	2
<u>Learning Outcomes</u>	2
<u>General Assessment Information</u>	3
<u>Assessment Tasks</u>	3
<u>Delivery and Resources</u>	5
<u>Unit Schedule</u>	7
<u>Policies and Procedures</u>	7
<u>Changes from Previous Offering</u>	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.

General Information

Unit convenor and teaching staff

Unit Convenor

Matthew Mansour

matthew.mansour@mq.edu.au

Refer to ilearn

Lecturer

Ed Moore

ed.moore@mq.edu.au

Refer to ilearn

Credit points

10

Prerequisites

Corequisites

Co-badged status

Unit description

This unit tackles cyber security as a multidisciplinary issue. It introduces information security and important technology concepts as well as cyber hygiene principles to remain safe in the digital world. It discusses cybercriminality (perpetrators and activities on the dark web) and its impact on society and prompts to critically think about the relationship between cyber security and privacy, from a legal standpoint. Finally, this unit provides insights into the cybersecurity risks faced by business and the role that risk management plays in addressing those risks in the context of corporate governance.

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 an understanding of technical concepts related to information security, computing, networking, and emerging technologies.

ULO2: Apply cyber hygiene principles to achieve personal security in the digital world.

ULO3: Report on cyber criminality (in terms of activities, perpetrators and their motives)

as well as its impact on society.

ULO4: Critically evaluate the relation between cyber security and privacy in the context of a legal and regulatory framework.

ULO5: Identify cybersecurity risks faced by business and relate the management of those risks to the enterprise governance.

General Assessment Information

General Faculty Policy on assessment submission deadlines and late submissions:

Online quizzes, in-class activities, or scheduled tests and exam must be undertaken at the time indicated in the unit guide. Should these activities be missed due to illness or misadventure, students may apply for Special Consideration.

All other assessments must be submitted by 5:00 pm on their due date.

Should these assessments be missed due to illness or misadventure, students should apply for Special Consideration.

Assessments not submitted by the due date will receive a mark of zero **unless** late submissions are specifically allowed as indicated in the unit guide or on iLearn.

If late submissions are permitted as indicated in the unit guide or on iLearn a consistent penalty will be applied for late submissions as follows:

A 12-hour grace period will be given after which the following deductions will be applied to the awarded assessment mark: 12 to 24 hours late = 10% deduction; for each day thereafter, an additional 10% per day or part thereof will be applied until five days beyond the due date. After this time, a mark of zero (0) will be given. For example, an assessment worth 20% is due 5 pm on 1 January. Student A submits the assessment at 1 pm, 3 January. The assessment received a mark of 15/20. A 20% deduction is then applied to the mark of 15, resulting in the loss of three (3) marks. Student A is then awarded a final mark of 12/20.

Assessment Tasks

Name	Weighting	Hurdle	Due
<u>In class assessment</u>	30%	No	Weeks 4/6/8/10/12
<u>Individual report</u>	30%	No	Week 7 (Fri 8th April @ 5pm)
<u>Final Take Home Essay.</u>	40%	No	TBA on ilearn

In class assessment

Assessment Type ¹: Presentation

Indicative Time on Task ²: 10 hours

Due: **Weeks 4/6/8/10/12**

Weighting: **30%**

This assessment task takes place in class (online or in class). It involves group work, debate and / or presentations. The Assessments happen on a fortnightly basis with the week prior being the preparation week. In order to complete the presentation you must be present in the preparation week also.

On successful completion you will be able to:

- Demonstrate an understanding of technical concepts related to information security, computing, networking, and emerging technologies.
- Apply cyber hygiene principles to achieve personal security in the digital world.
- Report on cyber criminality (in terms of activities, perpetrators and their motives) as well as its impact on society.
- Critically evaluate the relation between cyber security and privacy in the context of a legal and regulatory framework.

Individual report

Assessment Type **1**: Report

Indicative Time on Task **2**: 20 hours

Due: **Week 7 (Fri 8th April @ 5pm)**

Weighting: **30%**

The assessment task is to write a report with scholarly references that will address a contemporary topic relating to Cyber Security.

On successful completion you will be able to:

- Demonstrate an understanding of technical concepts related to information security, computing, networking, and emerging technologies.
- Apply cyber hygiene principles to achieve personal security in the digital world.
- Report on cyber criminality (in terms of activities, perpetrators and their motives) as well as its impact on society.
- Critically evaluate the relation between cyber security and privacy in the context of a legal and regulatory framework.
- Identify cybersecurity risks faced by business and relate the management of those risks to the enterprise governance.

Final Take Home Essay.

Assessment Type ¹: Essay

Indicative Time on Task ²: 20 hours

Due: **TBA on ilearn**

Weighting: **40%**

A final essay is included as an assessment task for this unit to provide assurance that: i) the product belongs to the student and ii) the student has attained the knowledge and skills from the unit. The student will have a short period of 72 hours to complete the essay.

On successful completion you will be able to:

- Demonstrate an understanding of technical concepts related to information security, computing, networking, and emerging technologies.
- Apply cyber hygiene principles to achieve personal security in the digital world.
- Report on cyber criminality (in terms of activities, perpetrators and their motives) as well as its impact on society.
- Critically evaluate the relation between cyber security and privacy in the context of a legal and regulatory framework.
- Identify cybersecurity risks faced by business and relate the management of those risks to the enterprise governance.

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

Teaching and Learning Strategy

COMP1300 is taught via Live lectures (in class) and streamed via Echo. Tutorials (Live on campus OR Live via Zoom - check timetables.mq.edu.au for which classes are on campus and which are online. NB You cannot mix modes). The feedback that you receive plays also a crucial role in your learning.

Lectures are used to introduce new material, give examples of the advances in Cyber Security and technologies and put them in a wider context. The unit is an introduction which in turn will be explored further in other units at Macquarie University.

Tutorials are small group classes which give you the opportunity to interact with your peers and with a tutor who has a sound knowledge of the subject. This also gives you a chance to practice your soft skills. **NB. For this semester for COMP1300, tutorials start in week 2 and the Lectures start in week 1.**

You have many opportunities to seek for and to receive feedback. During lectures, you are encouraged to ask the lecturer questions to clarify anything you might not be sure of.

Each week you should:

- Attend live lectures, take notes, ask questions
- Attend your tutorials and seek feedback from your tutor on your work
- Read assigned reading material, add to your notes and prepare questions for your lecturer or tutor
- Start working on any assessments immediately after they have been released.

Lecture notes are made available each week but these notes are intended as an outline of the lecture only and are not a substitute for your own notes or reading additional material.

Classes

Each week you should attend two hours of live lectures (via Zoom), and a one hour tutorial class (on campus OR online via Zoom)

Please note that you are **required** to submit a certain number of assessments. Failure to do so may result in you failing the unit.

Textbook.

Being a fast paced ever evolving unit, it was deemed that a textbook would not validate the complexity of Cyber Security. In turn we have used resources from 3 Faculties to give you as much exposure to Cyber Security and the real world.

Technology used and required

Echo

Digital recordings of lectures are available.

COMP1300 makes use of the following software in the lab:

- Microsoft Windows 10 +
- Microsoft Office 2016 +
- Edge or Mozilla Firefox or Chrome

Website

The web page for this unit can be found at: <http://ilearn.mq.edu.au>.

Student Support Services

Macquarie University provides a range of Academic Student Support Services. Details of these services can be accessed at <http://www.student.mq.edu.au>.

Assumed knowledge

Basic computer use skills.

Unit Schedule

Week	Lecture Topics/Events	Assessments
1	When... not if... <i>Intro to Cyber Security unit. (MM)</i>	Tutorials start in week 2 Lectures start in week 1
2	Cyber Hygiene – <i>How clean are you? (MM)</i>	Practice in_class assessment – Data Breach Poster
3	The Human Factor (MM)	In class assessment - Prep week
4	Basics of Protection (EM)	In class assessment - Presentation week
5	Computing Basics for Cyber Security (EM)	In class assessment - Prep week
6	Societal Security (MM)	In class assessment - Presentation week
7	Impact on Business and Cyber Governance – <i>Who's loses their job? (MM)</i>	In class assessment - Prep week & Individual Report Due : Fri 8th Apr @ 5pm
8	Cybercrime / Cybercriminal's (EM)	In class assessment - Presentation week
9	Cryptography (MM)	In class assessment - Prep Week
10	IoT and Emerging Tech (MM)	In class assessment - Presentation Week
11	Industry Experts (MM)	In class assessment - Prep Week
12	The Future – How is Cyber Security going to impact us (EM)	In class assessment - Presentation Week
13	Discussion about the Final Exam (MM)	Wrap up and Cyber Security Ethics Simulation

Policies and Procedures

Macquarie University policies and procedures are accessible from [Policy Central \(https://policies.mq.edu.au\)](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](#)
- [Assessment Procedure](#)
- [Complaints Resolution 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) (<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) (<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

Academic Integrity

At Macquarie, we believe [academic integrity](#) – honesty, respect, trust, responsibility, fairness and courage – is at the core of learning, teaching and research. We recognise that meeting the expectations required to complete your assessments can be challenging. So, we offer you a range of resources and services to help you reach your potential, including free [online writing and maths support](#), [academic skills development](#) and [wellbeing consultations](#).

Student Support

Macquarie University provides a range of support services for students. For details, visit <http://students.mq.edu.au/support/>

The Writing Centre

[The Writing Centre](#) provides resources to develop your English language proficiency, academic writing, and communication skills.

- [Workshops](#)
- [Chat with a WriteWISE peer writing leader](#)

- [Access StudyWISE](#)
- [Upload an assignment to Studiosity](#)
- [Complete the 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

Macquarie University offers a range of [Student Support Services](#) including:

- [IT Support](#)
- [Accessibility and disability support](#) with study
- Mental health [support](#)
- [Safety support](#) to respond to bullying, harassment, sexual harassment and sexual assault
- [Social support](#) including information about finances, tenancy and legal issues

Student Enquiries

Got a question? Ask us via [AskMQ](#), or contact [Service Connect](#).

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 from Previous Offering

Updated material and Assessments.

New SC policy

Hybrid Lectures