# COMP6013

## Introduction to Cyber Security

Session 2, In person-scheduled-weekday, North Ryde 2024

*School of Computing*

## Contents

**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
Convenor, Lecturer
Yimeng Feng
yimeng.feng@mq.edu.au
Contact via By email
TBA

Lecturer
Xiaohan Yu
xiaohan.yu@mq.edu.au
Contact via By email
TBA

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 cyber criminality (perpetrators and activities on the dark web), its
impact on society, and prompts for us 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 businesses 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 businesses and relate the management of those risks to enterprise governance.

# General Assessment Information

**Late Assessment Submission Penalty**

Unless a Special Consideration request has been submitted and approved, a 5% penalty (of the total possible mark of the task) will be applied for each day a written report or presentation assessment is not submitted, up until the 7th day (including weekends). After the 7th day, a grade of '0' will be awarded even if the assessment is submitted. The submission time for all uploaded assessments is 11:55 pm. A 1-hour grace period will be provided to students who experience a technical concern. For any late submission of time-sensitive tasks, such as scheduled tests/exams, performance assessments/presentations, and/or scheduled practical assessments/labs, students need to submit an application for Special Consideration.

**Special Consideration**

The Special Consideration Policy aims to support students who have been impacted by short-term circumstances or events that are serious, unavoidable and significantly disruptive, and which may affect their performance in assessment. If you experience circumstances or events that affect your ability to complete the assessments in this unit on time, please inform the convenor and submit a Special Consideration request through ask.mq.edu.au.

**Assessments where Late Submissions will be accepted**

In this unit, late submissions will be accepted as follows:

In class assessments, YES, Standard Late Penalty applies

Report, YES, Standard Late Penalty applies

Final Take Home Essay, YES, Standard Late Penalty applies

**Requirements to Pass this Unit**

To be eligible to pass this unit, it is necessary to obtain a mark of at least 50% in the unit overall.

# Assessment Tasks

| Name | Weighting | Hurdle | Due |
|------|-----------|--------|-----|
| Individual Report | 30% | No | Week 7 |

| Name | Weighting | Hurdle | Due |
|------|-----------|--------|-----|
| In-class assessment | 30% | No | Weeks 4/6/8/10/12 |
| Final take-home essay | 40% | No | Week 13 |

# Individual Report

Assessment Type [1]: Report
Indicative Time on Task [2]: 20 hours
Due: **Week 7**
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 businesses and relate the management of those risks to enterprise governance.

# 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.

# Final take-home essay

Assessment Type [1]: Essay
Indicative Time on Task [2]: 20 hours
Due: **Week 13**
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 businesses and relate the management of those risks to 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**

COMP6103 is taught via Live lectures (in class) and streamed via Echo. SGTA is taught via live classes on campus. The feedback that you receive in SGTA 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.

SGTA classes are small group classes which give you the opportunity to interact with your peers and with a SGTA instructor who has a sound knowledge of the subject. This also gives you a chance to practice your soft skills.

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.

**Week 1 classes**

SGTA classes start in week 1 and the Lectures start in week 1. Week 1 lecture will be on 22nd July 2024 (Monday).

Each week you should:

- Participate in live lectures, take notes, ask questions
- Participate in your SGTA classes and seek feedback from your SGTA instructor on your work
- Read assigned reading material, add to your notes and prepare questions for your lecturer or SGTA instructor
- 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 participate in two hours of live lectures and a one hour SGTA class (on campus).

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

**Methods of Communication**

We will communicate with you via your university email and through announcements on iLearn. Queries to convenors can either be placed on the iLearn discussion board or sent to the unit

convenor via the contact email on iLearn.

**Textbook**

Being a fast paced ever evolving unit, it was deemed that a textbook would not validate the complexity of Cyber Security.

**Technology used and required**

Echo

Digital recordings of lectures are available.

COMP6103 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 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… *Intro to Cyber Security unit. (MM)* | **SGTA classes start in week 1**<br><br>**Lectures start in week 1** |
| 2 | Cyber Hygiene – *How clean are you?* (MM) | Practice in_class assessment – Data Breach Poster |
| 3 | The Human Factor (MM) | In class assessment - Prep week |
| 4 | Basics of Protection and Computing Basics for Cyber Security (DV) | In class assessment - **Presentation week** |
| 5 | Cyber Security Management and Ethics Basics (DV) | In class assessment - Prep week |
| 6 | Societal Security (MM) | In class assessment - **Presentation week** |

| 7 | Impact on Business and Cyber Governance – *Who's loses their job?* (MM) | In class assessment - Prep week<br><br>**&**<br><br>**Individual Report Due : Friday 6th Sep @ 11.55pm** |
|---|---|---|
| 8 | Cybercrime / Cybercriminals ( DV) | In class assessment - **Presentation week** |
| 9 | Cryptography (DV) | In class assessment - Prep Week |
| 10 | IoT and Emerging Tech (DV) | 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 (DV) | In class assessment - **Presentation Week** |
| 13 | Discussion about the Final Report (MM / DV) | 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). 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). 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 connect.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 an d maths support, academic skills development and wellbeing consultations.

## Student Support

Macquarie University provides a range of support services for students. For details, visit http://stu dents.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 Advocacy provides independent advice on MQ policies, procedures, and

processes

## Student Enquiries

Got a question? Ask us via the Service Connect Portal, 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

We value student feedback to be able to continually improve the way we offer our units. As such we encourage students to provide constructive feedback via student surveys, to the teaching staff directly, or via the FSE Student Experience & Feedback link in the iLearn page.

Student feedback from the previous offering of this unit was very positive overall, with students pleased with the clarity around assessment requirements and the level of support from teaching staff. As such, no change to the delivery of the unit is planned, however we will continue to strive to improve the level of support and the level of student engagement.

Unit information based on version 2024.04 of the Handbook