COMP107

Introduction to Cyber Security

S1 Day 2019

Dept 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
Unit Convenor
Matthew Mansour
matthew.mansour@mq.edu.au
Check ilearn for details

Lecturer
Ed Moore
ed.moore@mq.edu.au
Check ilearn for details

Lecturer
Yvette Blount
yvette.blount@mq.edu.au
Check ilearn for details

Lecturer
Stephen McCombie
stephen.mccombie@mq.edu.au
Check ilearn for details

Credit points
3

Prerequisites

Corequisites

Co-badged status

Unit description
This unit tackles cyber security as a multidiscplinary 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:

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.

Assessment Tasks

Name	Weighting	Hurdle	Due
In class Participation	24%	Yes	Weeks 3-12
Quiz	12%	No	Week 6 in tutorial
Group Report + Video	24%	No	29/04/19
Final Exam	40%	No	Examination Period

In class Participation

Due: **Weeks 3-12**
Weighting: **24%**
This is a hurdle assessment task (see assessment policy for more information on hurdle assessment tasks)

In accordance with the Faculty Board all 100-level units in the Faculty will have a compulsory (hurdle) requirement on participation in tutorials, practicals and laboratories.

In-class voluntary participation will be assessed randomly for 10 tutorials during the session. The best 8 out of 10 in-class participation marks will be taken into consideration. I

Each week you will be working on different tasks that maybe and not limited to: Group Presentations, Quiz, Debates.

NB. This is a hurdle assessment, in order to pass the unit you will be required to participate in 8 out of the 10 weeks. If you receive any formal special consideration you will be given a waiver for that week. Please refer to https://students.mq.edu.au/study/my-

study-program/special-consideration

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.

Quiz

Due: **Week 6 in tutorial**
Weighting: **12%**

In class Quiz

In week 6 there will be a quiz in the tutorial.

The quiz will cover important parts of the unit material from weeks 1 - 5 and, as well as assessing your current level of mastery of it, give you and your tutor an opportunity to address any problem areas before the final exam. The quiz will normally not take the whole class and will be followed by in-class discussion. Please be on time to these classes, as the quiz will be the first thing in the class.

NB. In the circumstances that a public holiday falls on your workshop time for the quiz, you will being doing the quiz in the week following. More details will be provided on ilearn if required.

On successful completion you will be able to:

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

Group Report + Video

Due: **29/04/19**
Weighting: **24%**

The assessment task is to write a group report with scholarly references that will address a contemporary topic relating to Cyber Security. (**NB**. In addition you will have a reflection video component as part of the assessment as an individual. (full details are available on iLearn).

Submission

All reports will be submitted through Turnitin on iLearn and marked through grademark (the online marking system). Students will receive feedback within two weeks of the report submission through Grademark and Gradebook on the iLearn website.

Extensions

No extensions will be granted.

Penalty for Late Submission

No extensions will be granted. There will be a deduction of 10% of the total available marks made from the total awarded mark for each 24 hour period or part thereof that the submission is late (for example, 25 hours late in submission – 20% penalty). This penalty does not apply for cases in which an application for special consideration is made and approved (see https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policies/special-consideration). No submission will be accepted after solutions have been posted.

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 Exam

Due: **Examination Period**
Weighting: **40%**

A final examination 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 tested in the exam.

A two and a half (2.5) hour final examination for this unit will be held during the University Examination period.

Supplementary Exams

If a Supplementary Examination is granted as a result of the Special Consideration Policy the examination will be scheduled as per the Supplementary Examination timetable of the Faculty. Please note that the supplementary examination will be of the similar format as the final examination.

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.
- 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.

Delivery and Resources

Teaching and Learning Strategy

COMP107 is taught via lectures, tutorials (in practical labs). 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.

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 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 lectures, and a one hour tutorial class.

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 every 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.

COMP107 makes use of the following software in the lab:

- Microsoft Windows 10
- Microsoft Office 2016
- Internet Explorer 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.*	Get to know your tutor and class
2	Cybercriminal's - *Who is really running the show* (SMC)	Data Breach Poster
3	Cybercrime – *Are all crimes the same?*(SMC)	In class assessment
4	Societal Security (YB)	In class assessment

5	Impact on Business and Cyber Governance – *Who's loses their job?* (YB)	In class assessment
6	Computing Basics for Cyber Security (EM)	Quiz
7	Basics of Protection (MM)	In class assessment
8	Cyber Hygiene – *How clean are you?* (MM)	In class assessment
9	The Human Factor (MM)	In class assessment
10	Impact on Business and Cyber Governance – Who's loses their job? (SMC)	In class assessment
11	The Future – *How is Cyber Security going to impact us* (MM)	In class assessment
12	Guest Lecturer(s)	In class assessment
13	Revision of the entire unit for the final exam.	Revision

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
- Fitness to Practice Procedure
- Grade Appeal Policy
- Complaint Management Procedure for Students and Members of the Public
- Special Consideration Policy *(**Note:** The Special Consideration Policy is effective from 4 December 2017 and replaces the Disruption to Studies Policy.)*

Undergraduate 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/study/getting-started/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 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

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.

Graduate Capabilities

Creative and Innovative

Our graduates will also be capable of creative thinking and of creating knowledge. They will be imaginative and open to experience and capable of innovation at work and in the community. We want them to be engaged in applying their critical, creative thinking.

This graduate capability is supported by:

Learning outcome

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

Assessment tasks

- In class Participation
- Quiz
- Group Report + Video
- Final Exam

Capable of Professional and Personal Judgement and Initiative

We want our graduates to have emotional intelligence and sound interpersonal skills and to demonstrate discernment and common sense in their professional and personal judgement. They will exercise initiative as needed. They will be capable of risk assessment, and be able to handle ambiguity and complexity, enabling them to be adaptable in diverse and changing environments.

This graduate capability is supported by:

Learning outcomes

- 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.

Assessment tasks

- In class Participation
- Quiz
- Group Report + Video
- Final Exam

Discipline Specific Knowledge and Skills

Our graduates will take with them the intellectual development, depth and breadth of knowledge, scholarly understanding, and specific subject content in their chosen fields to make them competent and confident in their subject or profession. They will be able to demonstrate, where relevant, professional technical competence and meet professional standards. They will be able to articulate the structure of knowledge of their discipline, be able to adapt discipline-specific knowledge to novel situations, and be able to contribute from their discipline to inter-disciplinary solutions to problems.

This graduate capability is supported by:

Learning outcomes

- 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.

Assessment tasks

- In class Participation
- Quiz
- Group Report + Video
- Final Exam

Critical, Analytical and Integrative Thinking

We want our graduates to be capable of reasoning, questioning and analysing, and to integrate and synthesise learning and knowledge from a range of sources and environments; to be able to critique constraints, assumptions and limitations; to be able to think independently and systemically in relation to scholarly activity, in the workplace, and in the world. We want them to have a level of scientific and information technology literacy.

This graduate capability is supported by:

Learning outcomes

- Demonstrate an understanding of technical concepts related to information security, computing, networking, and emerging technologies.
- Identify cybersecurity risks faced by business and relate the management of those risks to the enterprise governance.

Assessment tasks

- In class Participation
- Quiz
- Group Report + Video
- Final Exam

Problem Solving and Research Capability

Our graduates should be capable of researching; of analysing, and interpreting and assessing data and information in various forms; of drawing connections across fields of knowledge; and they should be able to relate their knowledge to complex situations at work or in the world, in order to diagnose and solve problems. We want them to have the confidence to take the initiative in doing so, within an awareness of their own limitations.

This graduate capability is supported by:

Learning outcomes

- 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.

Assessment tasks

- In class Participation
- Quiz
- Group Report + Video
- Final Exam

Effective Communication

We want to develop in our students the ability to communicate and convey their views in forms effective with different audiences. We want our graduates to take with them the capability to read, listen, question, gather and evaluate information resources in a variety of formats, assess, write clearly, speak effectively, and to use visual communication and communication technologies as appropriate.

This graduate capability is supported by:

Learning outcomes

- 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.
- 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.

Assessment tasks

- In class Participation
- Quiz
- Group Report + Video
- Final Exam

Engaged and Ethical Local and Global citizens

As local citizens our graduates will be aware of indigenous perspectives and of the nation's historical context. They will be engaged with the challenges of contemporary society and with knowledge and ideas. We want our graduates to have respect for diversity, to be open-minded, sensitive to others and inclusive, and to be open to other cultures and perspectives: they should have a level of cultural literacy. Our graduates should be aware of disadvantage and social justice, and be willing to participate to help create a wiser and better society.

This graduate capability is supported by:

Learning outcomes

- Demonstrate an understanding of technical concepts related to information security, computing, networking, and emerging technologies.
- Report on cyber criminality (in terms of activities, perpetrators and their motives) as well as its impact on society.

Assessment tasks

- In class Participation
- Quiz
- Group Report + Video
- Final Exam

Socially and Environmentally Active and Responsible

We want our graduates to be aware of and have respect for self and others; to be able to work with others as a leader and a team player; to have a sense of connectedness with others and country; and to have a sense of mutual obligation. Our graduates should be informed and active participants in moving society towards sustainability.

This graduate capability is supported by:

Learning outcome

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

Assessment tasks

- In class Participation
- Group Report + Video
- Final Exam

Changes from Previous Offering

This is our inaugural semester.

Changes since First Published

Date	Description
19/02/2019	The major report had the date of 29/05/19 and should be: 29/04/19, so small typo