ACCG3025

Cyber Security and Privacy

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

Department of Actuarial Studies and Business Analytics

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
Mauricio Marrone
accg3025@mq.edu.au
See iLearn for consultation hours

Credit points
10

Prerequisites
130cp at 1000 level or above

Corequisites

Co-badged status

Unit description
Cyber-security and privacy are two of the biggest issues facing businesses operating in the Information Age. This unit explores how businesses both face and respond to such threats and opportunities as they integrate the Internet into their existing operations and new products/technologies in Australia and internationally. This unit is designed to give students practical skills to identify and mitigate those cyber-security and privacy risks, and to resolve legal disputes that may emerge from them, whether as a manager, an employee, or as an external consultant.

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: Identify and synthesise cybersecurity risks facing modern businesses

ULO2: Analyse practical implications of different theories about privacy and governance strategies necessary for effective business leadership both before and after a cyber-attack

ULO3: Apply Australian and foreign laws and ethics to determine how businesses can build trust through managing personal information and confidential business information

ULO4: Evaluate privacy risks through applying Privacy Impact Assessment methodologies for existing and new products/processes within a business

General Assessment Information

Late Assessment Submission Penalty (written assessments)

Unless a Special Consideration request has been submitted and approved, a 5% penalty (of the total possible mark) will be applied each day a written 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. Submission time for all written assessments is set at 11.55pm. A 1-hour grace period is provided to students who experience a technical concern.

For any late submissions 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.

All other submissions (Privacy Hot Topic Debate and Reflections of Cybersecurity Breach Response) will happen within your assigned tutorials. Students must be present to be eligible to submit their work. If they are unable to attend the tutorial, a special consideration must be submitted and approved.

Assessment Tasks

Name	Weighting	Hurdle	Due
Privacy Hot Topic Debate	20%	No	Video: Wk9 (15%) / Rebuttal Wk10 (5%) During Tutorial
Cybersecurity Breach Response	40%	No	Reflections:Wk4/5/6 (4% each). Report:Wk7 Fri 11:55pm (28%)
Privacy Impact Assessment	40%	No	Week 13 - Friday at 11:55pm

Privacy Hot Topic Debate

Assessment Type [1]: Debate
Indicative Time on Task [2]: 20 hours
Due: **Video: Wk9 (15%) / Rebuttal Wk10 (5%) During Tutorial**
Weighting: **20%**

Students will debate a current privacy business problem / challenge. Students will prepare a 6-10 minute video of their ethical, financial and legal arguments for- or against - the matter and upload their video to iLearn. Each student will then be randomly allocated to another (opposing) student's video to which they will prepare a short rebuttal video which they will also upload to iLearn.

On successful completion you will be able to:

- Analyse practical implications of different theories about privacy and governance strategies necessary for effective business leadership both before and after a cyber-attack
- Apply Australian and foreign laws and ethics to determine how businesses can build trust through managing personal information and confidential business information

Cybersecurity Breach Response

Assessment Type [1]: Report
Indicative Time on Task [2]: 35 hours
Due: **Reflections:Wk4/5/6 (4% each). Report:Wk7 Fri 11:55pm (28%)**
Weighting: **40%**

Acting in the role of a Chief Information Security Officer for a company that has just suffered a major cybersecurity attack, each student will prepare a report to the Board of Directors of the company advising what the vulnerabilities were in the business and what the company should do in response to the attack.Length: 2,500-word.

On successful completion you will be able to:

- Identify and synthesise cybersecurity risks facing modern businesses
- Analyse practical implications of different theories about privacy and governance strategies necessary for effective business leadership both before and after a cyber-attack
- Apply Australian and foreign laws and ethics to determine how businesses can build trust through managing personal information and confidential business information

Privacy Impact Assessment

Assessment Type [1]: Report
Indicative Time on Task [2]: 35 hours
Due: **Week 13 - Friday at 11:55pm**
Weighting: **40%**

Each student will prepare a privacy impact assessment of the risks and opportunities that exist in a proposed new business activity. Length: 2,500-word.

On successful completion you will be able to:

- Analyse practical implications of different theories about privacy and governance strategies necessary for effective business leadership both before and after a cyber-attack
- Apply Australian and foreign laws and ethics to determine how businesses can build trust through managing personal information and confidential business information
- Evaluate privacy risks through applying Privacy Impact Assessment methodologies for existing and new products/processes within a business

[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

Required Text:	Required Texts: As Cyber Security and Privacy are fast-moving topics, a textbook will likely be significantly outdated by the time it reaches print. Consequently, there will be no prescribed textbook.
Unit Web Page:	Available on iLearn
Technology Used and Required:	Students will require access to a computer and the Internet to undertake research and prepare their answers for their assessment tasks. You will need a mobile phone with a camera (or equivalent) to record your debate videos.
Delivery format and other details:	Lectures: Pre-recorded lectures will constitute the first hour of the class, with the second hour being a consultation/ catchup with the UC. The timetable for classes can be found on the University website at: http://timetables.mq.edu.au Students must attend all tutorials. Students must attend the tutorial in which they are enrolled and may not change tutorials without the prior permission of the course convenor.

Recommended Readings:	There are many cybersecurity and privacy sources of information online. A few worth looking at include: • SecurityAffairs: http://securityaffairs.co/wordpress/ • Krebs on Security: https://krebsonsecurity.com/
Other Course Materials:	Will be made available on iLearn
Workload:	See table below. This unit comprises 13 weekly lectures and 12 tutorials (no tutorial in week 1). Many tutorials will require active participation in small group exercises.

Activity	**Hours**
Cybersecurity Breach Response	35
Privacy Hot Topic Video Debate	20
Privacy Impact Assessment	35
Classes & Class Preparation	60
Total	150

Unit Schedule

The schedule below is indicative of the topics we will cover.

Week	Lecture Topic
1	Cyber-security and privacy
2	Exploits and defenses
3	Motives, Methods and Malicious Minds
4	Identifying risks, frameworks and tools
5	Responding to Cyber-security attacks
6	Business roles involvement in minimising cyber-security issues
7	Obligations and safeguarding the digital domain
Break	
8	Minimising threats as an individual

9	Privacy in Australia
10	Assessing privacy compliance in businesses
11	Assessing privacy risks in new technologies/businesses
12	Guest Lecturer - Contemporary cyber-security topics
13	Course Review: Engaging with the inherent tensions between cyber-security and privacy

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 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 Advocacy provides independent advice on MQ policies, procedures, and processes

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.

General Assessment Information

Late Assessment Submission Penalty (written assessments)

Unless a Special Consideration request has been submitted and approved, a 5% penalty (of the total possible mark) will be applied each day a written 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. Submission time for all written assessments is set at 11.55pm. A 1-hour grace period is provided to students who experience a technical concern.

For any late submissions 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.

Unit information based on version 2024.03 of the Handbook