ACCG3025

Cyber Security and Privacy

Session 2, Weekday attendance, North Ryde 2021

Department of Accounting & Corporate Governance

Contents

Session 2 Learning and Teaching Update

The decision has been made to conduct study online for the remainder of Session 2 for all units WITHOUT mandatory on-campus learning activities. Exams for Session 2 will also be online where possible to do so.

This is due to the extension of the lockdown orders and to provide certainty around arrangements for the remainder of Session 2. We hope to return to campus beyond Session 2 as soon as it is safe and appropriate to do so.

Some classes/teaching activities cannot be moved online and must be taught on campus. You should already know if you are in one of these classes/teaching activities and your unit convenor will provide you with more information via iLearn. If you want to confirm, see the list of units with mandatory on-campus classes/teaching activities.

Visit the MQ COVID-19 information page for more detail.

General Information

Unit convenor and teaching staff
Unit Convenor
Matthew Mansour
matthew.mansour@mq.edu.au
Contact via accg3025@mq.edu.au
Via Zoom - Check on ilearn for more details

Moderator
Yvette Blount
accg3025@mq.edu.au - students are not to email the moderator

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

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

How Feedback will be provided to you on your performance in your Assessment Tasks: A marking rubric will be provided to you which will deliver feedback to you on your performance in your Report on Employee Culture, your Ransomware Debate Videos and your Privacy Impact Assessment. The marking rubrics can be found in the turnitin submission links when available.

Late Submission(s): Late assessment must also be submitted through Turnitin. 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 incurs a 20% penalty). Late submissions will not be accepted after solutions have been discussed and/or made available. This penalty does not apply for cases in which an application for Special Consideration is made and approved. Note: applications for Special Consideration Policy must be made within 5 (five) business days of the due date and time.

Self-Plagiarism: Macquarie's plagiarism policy (see link below) does not allow this, there are no exemptions on similarity for these type of situations and the similarity number will only increase once both are in the Turnitin database and match with each other. Tread very carefully if this situation applies to you, your discussion points will have to be almost completely different in each unit. Consider this early fair warning.

https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policies/academic-integrity

Assessment Tasks

Name	Weighting	Hurdle	Due
Cybersecurity Breach Response	40%	No	Checkpoint Wk4/5/6 (4% each) Report due: Wk7(28%)
Privacy Hot Topic Debate	20%	No	Video: Wk9 (15%) / Rebuttal Wk10 (5%)
Privacy Impact Assessment	40%	No	Week 13

Cybersecurity Breach Response

Assessment Type [1]: Report
Indicative Time on Task [2]: 35 hours
Due: **Checkpoint Wk4/5/6 (4% each) Report due: Wk7(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 Hot Topic Debate

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

Privacy Impact Assessment

Assessment Type [1]: Report
Indicative Time on Task [2]: 35 hours
Due: **Week 13**
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

Coronavirus (COVID-19) Update

Any references to on-campus delivery below may no longer be relevant with the current situation in Sydney (Always check timetables.mq.edu.au for any updates and ilearn)

Required Text:	Required Texts: As Cyber Security and Privacy are such fast-moving topics, by the time it reaches print a textbook is likely to be significantly out of date. Consequently, there will be no prescribed textbook. Instead, required readings will be uploaded on ilearn.
Unit Web Page:	available on iLearn
Technology Used and Required:	Students will require access to a computer and to the Internet so as to undertake research and to prepare their answers for their assessment tasks. You will need a mobile phone with a camera or a GoPro (or equivalent) to record your debate videos. Software: iLearn, VLC Media Player, Microsoft Office, Adobe Acrobat Reader, Internet Browser, Email Client Software, Adobe Premiere Pro can be used to edit videos.
Delivery format and other details:	Lectures: There will be **pre-recorded** lectures that will constitute the first hour of the lecture with the second hour being a "live" consultation / catchup with the UC on Monday nights from 6 - 7pm. 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:	**Activity** / **Hours** Cybersecurity Breach Response: 35 Privacy Hot Topic Video Debate: 20 Privacy Impact Assessment: 35 Classes & Class Preparation: 60 Total: 150 This unit consists of 13 weekly lectures and 12 tutorials (no tutorial in week 1). Many tutorials will require active participation in small group exercises.
Inherent Requirements to complete the unit successfully?	Both individual work (on your assessment tasks) and group work (for your exercises in tutorials) are required to successfully complete this Unit. Students will need to be capable of: a) listening to the recorded lecture , attending consultation / catch up Mon 6-7pm b) actively engaging in tutorial exercises; and c) completing written and video tasks.

Unit Schedule

Week	Lecture Topic	Readings

1	Introduction: the Differences between Cyber-Security and Privacy	See Prescribed Readings on iLearn
2	The Supply of Cyber-Security Threats	See Prescribed Readings on iLearn
3	The Demand to Exploit Cyber-Security Threats	See Prescribed Readings on iLearn
4	Cyber-Security Legal Obligations	See Prescribed Readings on iLearn
5	Minimising Cyber-Security Threats in a Business	See Prescribed Readings on iLearn
6	How to Respond to Cyber-Security Attacks on a Business and Resolving Disputes which can Emerge from such an Attack	See Prescribed Readings on iLearn
7	What is Privacy and Why should it be Protected?	See Prescribed Readings on iLearn
Break		
8	Privacy Obligations in Australia at the state and federal levels	See Prescribed Readings on iLearn
9	International Privacy Obligations and Transferring Data Across Borders	See Prescribed Readings on iLearn
10	How to Assess Privacy Compliance in an existing Business	See Prescribed Readings on iLearn
11	How to Assess Privacy Risks in new technologies / businesses	See Prescribed Readings on iLearn
12	How to Respond to a Privacy Breach and Resolving Disputes which can Emerge from such a Breach	See Prescribed Readings on iLearn
13	Course Review: Engaging with the Inherent Tensions Between Cyber-Security and Privacy	Covers all weeks

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
- Grade Appeal Policy
- Complaint Management 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

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 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.

Changes from Previous Offering

Due to the rapid development of cybersecurity and privacy issues and events in the real-world, the content of this unit is updated each offering.

Due to the uncertainty over the extent to which the Covid-19 viral pandemic is affecting Macquarie University at various times, tutorials and lecture delivery formats may vary over the course of the semester in accordance with the University's health and safety advice.

Research and Practice, Global & Sustainability

This unit uses research from academic researching at Macquarie University, including:

- John Selby, How Businesses can Build Trust in the Face of Cybersecurity Risks: Optus-Macquarie Cybersecurity Hub Whitepaper (2017)
- John Selby, Data Localisation Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both? (2017) International Journal of Law & Information Technology

and numerous primary and secondary legal materials published through AUSTLII <http://www.austlii.edu.au> and other external sources.

The unit also builds upon the convenor's practical experience working as a lawyer resolving privacy disputes and advising on cybersecurity risks, and presentations he has made to the United Nations Internet Governance Forum on cybercrime and cybersecurity issues. The convenor attended a GDPR training course in Brussels.