ACCG3060

Cyber Security Governance and Ethics

Session 1, Weekday attendance, North Ryde 2020

Department of Accounting & Corporate Governance

Contents

General Information

Unit convenor and teaching staff
Unit Convenor, Lecturer, Tutor
John Selby
john.selby@mq.edu.au
Contact via 9850 7081
4 Eastern Road, Level 3, Room 353
Tuesdays 2-3pm

Moderator
Yvette Blount
yvette.blount@mq.edu.au - students are not to email Dr Blount

Credit points
10

Prerequisites
((ACCG250 or ACCG2050) and ACCG2065) or PICT201 or PICT2001

Corequisites

Co-badged status

Unit description
Every person in an organisation is responsible for safe guarding customer data in this era of increasing cyber threats. This unit is designed for students to gain an understanding of the regulatory environment, governance (including cyber governance) and ethical issues relating to cyber security. The objective of the unit is for students to understand the governance and ethical issues in the constantly evolving cyber security environment created by new digital technologies.

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: Explain the governance principles and ethical frameworks relevant to cyber security in a business context.

ULO2: Demonstrate well-reasoned judgement when critically analysing cyber security governance and ethical challenges.
ULO3: Evaluate how trade-offs between cyber security, cost/resources and business opportunities/competitive advantage intersect with risk tolerance, good corporate governance, and business ethics.
ULO4: Apply governance principles and ethical frameworks to develop solutions to a variety of governance and ethical challenges relating to cyber security in a range of business contexts.

Assessment Tasks

Coronavirus (COVID-19) Update

Assessment details are no longer provided here as a result of changes due to the Coronavirus (COVID-19) pandemic.

Students should consult iLearn for revised unit information.

Find out more about the Coronavirus (COVID-19) and potential impacts on staff and students

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 Algorithmic Impact Assessment. The marking rubrics can be found in your ACCG3060 Assessment Guide.

Students should also consult the Assessment Guide (available on iLearn) for more information about these assessment tasks.

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.

Delivery and Resources

Coronavirus (COVID-19) Update

Any references to on-campus delivery below may no longer be relevant due to COVID-19.

Please check here for updated delivery information: https://ask.mq.edu.au/account/pub/display/unit_status

Required Text:	Required Texts: As Cyber Security is such a fast-moving topic, 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 have been uploaded onto 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:	Students are required to attend a 1-hour lecture and 2-hour tutorial each week (Tutorials start in Week 2). 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 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

Activity	Hours
Organisational Culture & Cyber Security Report	35
Video Debate	20
Algorithmic 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.

Prize:	At present, there is not a cash Unit Prize for this unit.

Inherent Requirements to complete the unit successfully?

Both individual work (on your assessment tasks) and group work (for your practical exercises in tutorials) are required to successfully complete this Unit. Students will need to be capable of: a) attending lectures and/or listening to recordings of those lectures, b) actively engaging in practical tutorial exercises; and c) completing written and video tasks.

Unit Schedule

Coronavirus (COVID-19) Update

The unit schedule/topics and any references to on-campus delivery below may no longer be relevant due to COVID-19. Please consult iLearn for latest details, and check here for updated delivery information: https://ask.mq.edu.au/account/pub/display/unit_status

Week	Module	Topic
1		Introduction & Course Overview
2	Cyber Security Governance:	The Basics of Cyber Security Governance & its Regulatory Environment
3		Cyber Security Governance: ISO27001 & 27002
4		Organisational Culture and Cyber Security
5		Risk Transfer Through Cyber-Insurance
6	Cyber Security Ethical Decision-making:	Hacking Back & Ethical Responses to Ransomware Demands
7		Cyber (In-)Security by Design: Internet of Things Devices
8		Ethics of Surveillance Capitalism
9		Tracking Users Online Browsing for Marketing Purposes & Malware-vertising
10		Artificial Intelligence & its role in Cyber Security
11		AI Risks, including Algorithmic Bias
12		Algorithmic Impact Assessments
13		Conclusion

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.)*

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 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

This unit is being offered for the first time in 2020.