ACCG886

Cyber Security, Governance Frameworks and Ethics

S1 Evening 2019

Dept of Accounting & Corporate Governance

Contents

General Information

Unit convenor and teaching staff
Unit Convenor
Yvette Blount
accg886@mq.edu.au
Contact via accg886@mq.edu.au
Room 341 Level 3, 4 Eastern Road
4:00pm to 5:45pm Monday (before class)

Moderator
Mauricio Marrone
accg886@mq.edu.au
Contact via accg886@mq.edu.au

Credit points
4

Prerequisites
Admission to MCyberSec

Corequisites

Co-badged status

Unit description
Organisations have an ethical and legal responsibility to safeguard customer data in a constantly evolving cyber security environment. This unit is designed for students to gain an understanding of cyber security governance frameworks and ethical issues relating to the complex issues relating to cyber security. The primary objectives of the unit are for students to be able to evaluate cyber security trade-offs, use relevant governance frameworks to develop a cyber security road map and to be able to examine and provide recommendations for cyber security ethical dilemmas.

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:

Evaluate the trade-offs between cybersecurity, cost/resources and business

opportunities/competitive advantage

Develop a cybersecurity road map for a specific organisation.

Explain the governance principles and frameworks relevant to cybersecurity.

Examine and provide recommendations for potential ethical dilemmas of the work of cybersecurity experts

Assessment Tasks

Name	Weighting	Hurdle	Due
Contributions to discussions	30%	No	Weeks 3 to 12 (10 weeks)
Cybersecurity Roadmap/plan	30%	No	Week 7
Ethical Dilemmas Report	40%	No	Week 12

Contributions to discussions

Due: **Weeks 3 to 12 (10 weeks)**
Weighting: **30%**

This assessment includes contributions to discussions around cybersecurity issues relating to governance, management and ethics. Details and rubric are available on the iLearn website.

A variety of activities will be assigned each week from weeks 3 to 12 completed online or in class. Students are expected to complete readings and research as required prior to the class (available on the iLearn website).

Extensions

No extensions will be granted. Students who have not submitted the task prior to the deadline will be awarded a mark of 0 for the task, except 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).

Penalty for Late Submission

Not applicable

On successful completion you will be able to:

- Evaluate the trade-offs between cybersecurity, cost/resources and business opportunities/competitive advantage
- Develop a cybersecurity road map for a specific organisation.
- Explain the governance principles and frameworks relevant to cybersecurity.
- Examine and provide recommendations for potential ethical dilemmas of the work of cybersecurity experts

Cybersecurity Roadmap/plan

Due: **Week 7**
Weighting: **30%**

This assessment task is to develop a strategic cybersecurity roadmap/plan for the Board for a specific organisation. Details and marking rubric are available on the iLearn website.

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

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:

- Evaluate the trade-offs between cybersecurity, cost/resources and business opportunities/competitive advantage
- Develop a cybersecurity road map for a specific organisation.

Ethical Dilemmas Report

Due: **Week 12**
Weighting: **40%**

Report on ethical dilemmas for cybersecurity experts. Details and marking rubric are available on the iLearn website.

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

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:

- Explain the governance principles and frameworks relevant to cybersecurity.
- Examine and provide recommendations for potential ethical dilemmas of the work of cybersecurity experts

Delivery and Resources

Classes

There is one three (3) hour class (workshop) each week. The timetable is available here: https://timetables.mq.edu.au/2019/.

Students are expected to complete any pre-reading or other assigned activities prior to coming to class. The classes will consist of interactive activities including case studies and working in groups.

Textbook

Antonucci, D., 2017. *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*. John Wiley & Sons.(https://onlinelibrary.wiley.com/doi/book/10.1002/9781119309741)

Technology Used

Course material is available on the course website (https://www.mq.edu.au/iLearn/). Written assessment tasks are submitted through Turnitin. Access to the library website and other internet resources will be necessary to complete this unit.

Expectations and Workload

Students are expected to spend around 150 hours on this unit. Students should make a serious attempt on each of the assessment task to successfully meet the unit outcomes. As a guide students should expect to spend the time allocated on the following tasks:

	Activities	Hours
1	Weekly Classes	39
2	Weekly preparation (before class) approximately 2 hours per week	26
3	Contribution to discussions (assessed coursework)	25

4	Develop a strategic cyber security roadmap/plan for the Board (report)	25
5	Report on ethical dilemmas for cyber security experts (report)	35
	Total	150

Unit Schedule

Week	Topic	Readings
1	A Whole of Organisation Response to Cybersecurity	Chapters 1& 2
2	Governance Frameworks and Standards (1)	Chapters 3, 6, 15 & 22
3	Governance Frameworks and Standards (2)	Chapters 3, 6, 15 & 22
4	Policies and Procedures: Operations and Communications	Chapters 4 & 21
5	Culture and People (1)	Chapters 16, 24, 25 & 26
6	Culture and People (2)	Chapters 16, 24, 25 & 26
7	Analysing and Treating Cyber Risks (1)	Chapters 7,8,9 &10
8	Analysing and Treating Cyber Risks (2)	Chapters 7,8,9 &10

9	Legal and Compliance	Chapter 17
10	Cybersecurity Ethics	Readings: 1. Martin, C.D., 2017. TAKING THE HIGH ROAD White hat, black hat: the ethics of cybersecurity. ACM Inroads, 8(1), pp.33-35. 2. Francine Berman and Vinton G. Cerf. 2017. Social and ethical behavior in the internet of things. Commun. ACM 60, 2 (January 2017), 6-7. DOI: https://doi.org/10.1145/3036698 3. By Knowles, Aidan 2016 Tough Challenges in Cybersecurity Ethics - Security Intelligence https://securityintelligence.com/tough-challenges-cybersecurity-ethics/
11	Assurance and Cyber risk management	Chapter 18
12	Current Issues in Cyber security	Latest whitepapers, case studies
13	The future (strategic cyber security – IoT, Cloud, AI….)	TBA

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

PG - Capable of Professional and Personal Judgment and Initiative

Our postgraduates will demonstrate a high standard of discernment and common sense in their professional and personal judgment. They will have the ability to make informed choices and decisions that reflect both the nature of their professional work and their personal perspectives.

This graduate capability is supported by:

Learning outcome

- Evaluate the trade-offs between cybersecurity, cost/resources and business opportunities/competitive advantage

PG - Discipline Knowledge and Skills

Our postgraduates will be able to demonstrate a significantly enhanced depth and breadth of knowledge, scholarly understanding, and specific subject content knowledge in their chosen fields.

This graduate capability is supported by:

Learning outcomes

- Evaluate the trade-offs between cybersecurity, cost/resources and business opportunities/competitive advantage
- Develop a cybersecurity road map for a specific organisation.
- Explain the governance principles and frameworks relevant to cybersecurity.
- Examine and provide recommendations for potential ethical dilemmas of the work of cybersecurity experts

Assessment tasks

- Contributions to discussions
- Cybersecurity Roadmap/plan
- Ethical Dilemmas Report

PG - Critical, Analytical and Integrative Thinking

Our postgraduates will be capable of utilising and reflecting on prior knowledge and experience, of applying higher level critical thinking skills, and of integrating and synthesising learning and knowledge from a range of sources and environments. A characteristic of this form of thinking is the generation of new, professionally oriented knowledge through personal or group-based critique of practice and theory.

This graduate capability is supported by:

Learning outcome

- Evaluate the trade-offs between cybersecurity, cost/resources and business opportunities/competitive advantage

Assessment task

- Contributions to discussions

PG - Research and Problem Solving Capability

Our postgraduates will be capable of systematic enquiry; able to use research skills to create new knowledge that can be applied to real world issues, or contribute to a field of study or practice to enhance society. They will be capable of creative questioning, problem finding and problem solving.

This graduate capability is supported by:

Learning outcome

- Develop a cybersecurity road map for a specific organisation.

Assessment tasks

- Cybersecurity Roadmap/plan
- Ethical Dilemmas Report

PG - Effective Communication

Our postgraduates will be able to communicate effectively and convey their views to different social, cultural, and professional audiences. They will be able to use a variety of technologically supported media to communicate with empathy using a range of written, spoken or visual formats.

This graduate capability is supported by:

Learning outcomes

- Develop a cybersecurity road map for a specific organisation.
- Explain the governance principles and frameworks relevant to cybersecurity.
- Examine and provide recommendations for potential ethical dilemmas of the work of cybersecurity experts

Assessment tasks

- Contributions to discussions
- Cybersecurity Roadmap/plan
- Ethical Dilemmas Report

PG - Engaged and Responsible, Active and Ethical Citizens

Our postgraduates will be ethically aware and capable of confident transformative action in relation to their professional responsibilities and the wider community. They will have a sense of connectedness with others and country and have a sense of mutual obligation. They will be able to appreciate the impact of their professional roles for social justice and inclusion related to national and global issues

This graduate capability is supported by:

Learning outcomes

- Explain the governance principles and frameworks relevant to cybersecurity.
- Examine and provide recommendations for potential ethical dilemmas of the work of cybersecurity experts

Changes from Previous Offering

This is the first offering of the Unit