



BUSL315

Cyber-security & Privacy: Implications for Business & Law

S2 Day 2017

Dept of Accounting & Corporate Governance

Contents

<u>General Information</u>	2
<u>Learning Outcomes</u>	2
<u>General Assessment Information</u>	3
<u>Assessment Tasks</u>	3
<u>Delivery and Resources</u>	5
<u>Unit Schedule</u>	6
<u>Policies and Procedures</u>	7
<u>Graduate Capabilities</u>	9
<u>Changes from Previous Offering</u>	11
<u>Research and Practice, Global & Sustainability</u>	11

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, Lecturer & Tutor

John Selby

john.selby@mq.edu.au

Contact via john.selby@mq.edu.au

E4A 325

Wednesdays: 11am-noon; 2-3pm

Moderator

Dr Kay-Wah Chan

Credit points

3

Prerequisites

39cp

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:

Identify and synthesise cybersecurity risks facing modern businesses

Analyse governance strategies necessary for effective business leadership both before and after a cybersecurity attack

Analyse the practical implications of different theories about privacy

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

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

General Assessment Information

As they are each slightly different for each task, see above for specific information about submission methods, late submission options, extensions, penalties, etc for each assessment task.

Assessment Tasks

Name	Weighting	Hurdle	Due
<u>Tutorial Participation</u>	10%	No	ongoing
<u>Cybersecurity Breach Response</u>	40%	No	4.30pm on Thursday of Week 8
<u>Privacy Impact Assessment</u>	50%	No	4.30pm on Thursday of Week 13

Tutorial Participation

Due: **ongoing**

Weighting: **10%**

Active participation in the tutorial activities is expected each week. You must prepare for your tutorials in advance. Mere attendance will not gain you participation marks. You will be assessed in accordance with the Grading Policy and the marking rubric will be available on iLearn.

Failure to attend or participate in three or more tutorials during weeks 2-13 of the semester will result in a deduction from your tutorial participation mark of 1% (out of 10%) for each tutorial absence. No extensions will be granted, except in accordance with the Disruption Policy

This task is expected to take 24 hours.

On successful completion you will be able to:

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

existing and new products/processes within a business

Cybersecurity Breach Response

Due: **4.30pm on Thursday of Week 8**

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 a company advising what the vulnerabilities were in the business and what the company should do in response to the attack.

No extensions will be granted, except in accordance with the Disruption Policy.

There will be a deduction of 10% of the total available marks from the total awarded marks 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 is made and approved under the Disruption Policy.

This task is expected to take 60 hours.

On successful completion you will be able to:

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

Privacy Impact Assessment

Due: **4.30pm on Thursday of Week 13**

Weighting: **50%**

Each student will prepare a Privacy Impact Assessment of the risks and opportunities that exist in a proposed new business activity.

No extensions will be granted, except in accordance with the Disruption Policy.

There will be a deduction of 10% of the total available marks from the total awarded marks 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 is made and approved under the Disruption Policy.

This task is expected to take 66 hours.

On successful completion you will be able to:

- Analyse the practical implications of different theories about privacy
- Apply Australian and foreign laws and ethics to determine how businesses can build trust

through managing personal information & confidential business information

- Evaluate privacy risks through applying Privacy impact Assessment methodologies for existing and new products/processes within a business

Delivery and Resources

Classes:

1 x 2-hour face-to-face lecture and 1 x 1-hour in-person tutorial per week

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

Prizes:

A Macquarie University Accounting and Corporate Governance Prize is available for the highest achieving student in this unit: http://www.businessandconomics.mq.edu.au/undergraduate_degrees/prizes_scholarships

Required and Recommended Texts and/or Materials:

Required Texts: As Cybersecurity 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 onto iLearn.

Technology Used and Required

Access to a Personal Computer with Broadband Internet Access

iLearn, Microsoft Powerpoint, VLC Media Player/

Microsoft Office, Internet Browser, Email Client Software.

Unit Web Page:

Course material is available on the learning management system (iLearn)

Other than iLearn, there is no web page for this unit

Teaching and Learning Strategy:

This unit consists of 13 weekly online video 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 cybersecurity breach report and privacy impact assessment) 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 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](#). Students should be aware of the following policies in particular with regard to Learning and Teaching:

Academic Honesty Policy http://mq.edu.au/policy/docs/academic_honesty/policy.html

Assessment Policy http://mq.edu.au/policy/docs/assessment/policy_2016.html

Grade Appeal Policy <http://mq.edu.au/policy/docs/gradeappeal/policy.html>

Complaint Management Procedure for Students and Members of the Public http://www.mq.edu.au/policy/docs/complaint_management/procedure.html

Disruption to Studies Policy (in effect until Dec 4th, 2017): http://www.mq.edu.au/policy/docs/disruption_studies/policy.html

Special Consideration Policy (in effect from Dec 4th, 2017): <https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policies/special-consideration>

In addition, a number of other policies can be found in the [Learning and Teaching Category](#) of 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/support/student_conduct/

Results

Results shown in *iLearn*, 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.

All final grades in the Department of Accounting and Corporate Governance are determined by a grading committee and are not the sole responsibility of the Unit Coordinator.

Students will be awarded one of these grades. The final grade that is awarded reflects the corresponding grade descriptor in the Grading Policy.

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](#)

Disruption to Studies Policy

The University is committed to equity and fairness in all aspects of its learning and teaching. It recognises that students may experience disruptions that adversely affect their academic performance in assessment activities. A Disruption to Studies policy exists to support students who experience serious and unavoidable disruption. The policy is available at: http://www.mq.edu.au/policy/docs/disruption_studies/policy.html

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

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.

Access to all student computing facilities within the Faculty of Business and Economics is restricted to authorised coursework for approved units. Student ID cards must be displayed in the locations provided at all times.

Students are expected to act responsibly when using University IT facilities. The following regulations apply to the use of computing facilities and online services:

- Accessing inappropriate

web sites or downloading inappropriate material is not permitted. • Material that is not related to coursework for approved units is deemed inappropriate. • Downloading copyright material without permission from the copyright owner is illegal, and strictly prohibited. Students detected undertaking such activities will face disciplinary action, which may result in criminal proceedings.

Non-compliance with these conditions may result in disciplinary action without further notice.

Students must use their Macquarie University email addresses to communicate with staff as it is University policy that the University issued email account is used for official University communication.

Graduate Capabilities

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

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

Assessment tasks

- Tutorial Participation
- Cybersecurity Breach Response
- Privacy Impact Assessment

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

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

Assessment tasks

- Tutorial Participation
- Cybersecurity Breach Response
- Privacy Impact Assessment

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

- Identify and synthesise cybersecurity risks facing modern businesses
- Analyse governance strategies necessary for effective business leadership both before and after a cybersecurity attack
- Apply Australian and foreign laws and ethics to determine how businesses can build trust through managing personal information & confidential business information
- Evaluate privacy risks through applying Privacy impact Assessment methodologies for existing and new products/processes within a business

Assessment tasks

- Tutorial Participation
- Cybersecurity Breach Response

- Privacy Impact Assessment

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

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

Assessment tasks

- Tutorial Participation
- Cybersecurity Breach Response
- Privacy Impact Assessment

Changes from Previous Offering

BUSL315 was previously offered as Business Disputes and Litigation. The content and assessment tasks in the unit for this session have changed from its previous offering.

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)

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 is undertaking an international collaborative research project to further explore those issues.