BUSL315

Cyber-security & Privacy: Implications for Business & Law

S2 Day 2019

Dept 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 john.selby@mq.edu.au
E4A 325
Thursdays 9am-10am; 1-2pm

Moderator - students should not contact A/P Ashiabor
Hope Ashiabor
hope.ashiabor@mq.edu.au
n/a

Credit points
3

Prerequisites
39cp at 100 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:

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

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 Tutorial Participation, your Cybersecurity Breach Response and your Privacy Impact Assessment. The marking rubrics can be found in your BUSL315 Assessment Guide.

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

Assessment Tasks

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

Tutorial Participation

Due: **ongoing**
Weighting: **10%**

Task Description: Tutorial Participation requires more than mere physical attendance in a tutorial. Students are expected to display knowledge that they have completed the required reading for a tutorial, and are prepared to ask and answer questions on scheduled topics. Tutorial participation will include a student's engagement with practical exercises within a tutorial. Type of Collaboration: Individual Submission Through your engagement and comments made during each tutorial. Format: See the Assessment Guide on iLearn for detailed criteria and information on Class Participation Length: This unit has twelve one-hour tutorials held weekly starting in Week 2. Inherent Task Requirements: Complete the readings and develop your own answers to the assigned questions prior to attending each weekly tutorial. Late Submission:
Penalty:

Other than where a relevant applicaiton pursuant to the Special Consideration Policy is approved, failure to attend without providing satisfactory evidence of at least nine of the twelve tutorials over the course of the semester will result in a reduction in your participation mark that would have been awarded for the participation you engagedin during the tutorials that you did attend.

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%**

Task Description: 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. Type of Collaboration: Individual Submission: See the Assessment Guide on iLearn for detailed criteria and information on this assessment task, which will be submitted through Turnitin on the BUSL315 iLearn page. Format: Written Length: 2000 words (excluding bibliography and footnotes) Inherent Task Requirements: Students must undertake extensive research so as to understand and analyse the relevant issues. Students must ensure their references comply with the Australian Guide to Legal Citation (4th Ed.) Late Submission:
No extensions will be granted, except in accordance with the Special Consideration 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.

How will feedback be provided on your answer to this assessment task:

Written feedback will be provided to you on your answer to this assessment task. That feedback is expected to be returned to you by the end of Week 10. See the marking rubric in the Assessment Guide for more details.

Workload for this assessment task:

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%**

Task Description: Each student will prepare a Privacy Impact Assessment of the risks and opportunities that exist in a proposed new business activity. Type of Collaboration: Individual Submission: Online via Turnitin / iLearn Format: Written Length: 2500-word answer Inherent Task Requirements: Students must undertake extensive research so as to understand and analyse the relevant issues. Students must ensure their references comply with the Australian Guide to Legal Citation (4th Ed.) Late Submission:
No extensions will be granted, except in accordance with the Special Consideration 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 Special Consideration Policy.

How will feedback be provided on your answer to this assessment task:

Written feedback will be provided to you on your answer to this assessment task. See the marking rubric in the Assessment Guide for more details. As this will be your final assessment task for the unit, in accordance with Departmental Policy, that feedback will be available for you to view by requesting (through BESS) access to a hard copy of your answer after your final grade for the unit has been released.

Workload for this assessment task:

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

Required Text:	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 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. Software: iLearn, VLC Media Player, Microsoft Office, Adobe Acrobat Reader, Internet Browser, Email Client Software.
Delivery format and other details:	Students are required to attend a 2-hour lecture and 1-hour tutorial each week (Tutorials start in Week 2). The unit explores cybersecurity issues first before delving into privacy issues, and then integrating those two fields. 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** Tutorial Participation — 24 Cybersecurity Breach Report — 60 Privacy Impact Assessment — 66 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:	The International Association of Privacy Professionals Australia and New Zealand Legacy Prize of $1000 will be awarded to the highest achieving student in this unit. For more information, see: http://www.businessandeconomics.mq.edu.au/undergraduate_degrees/prizes_scholarships

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

Learning and Teaching Activities

Lectures

Each weekly lecture runs for two hours. During that time, the Unit Convenor will present you with challenging issues relating to cybersecurity and privacy. You will have the opportunity to ask questions.

Tutorials

Tutorials in this unit are highly interactive. They include: a simulation of cybersecurity attacks; a simulation of a business responding to a data breach; a debate over whether privacy should be considered an economic right or a human right; and roleplaying consultancy interviews with clients.

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 (http

s://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

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

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.

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

As cybersecurity and privacy are such rapidly developing topics, some of the readings have been updated to include sources from this year.

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.