PICT311

Cyber Security in Practice

S2 Day 2019

Department of Security Studies and Criminology

Contents

General Information

Unit convenor and teaching staff
Unit Convenor
Ed Moore
ed.moore@mq.edu.au
By Appointment

Credit points
3

Prerequisites
39cp at 100 level or above

Corequisites

Co-badged status

Unit description
Computer systems and networks, and the applications that they support, are essential to information flows, economic transactions and critical infrastructure in the twenty-first century. This unit will present an overview of modern cyber security with reference to both public and private sector organisations. The unit will look at the motives and perpetrators of cybercrime. It will explore how individuals and organisations face specific threats from their use of technology and identify challenges in maintaining cyber and information security. It further examines the protective security measures required to protect physical and digital access to information through people, infrastructure and computer systems. The unit complements PICT111 which looks at non-traditional security threats in the twenty-first century.

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:

Demonstrate a comprehensive understanding of the key crime types and criminological issues which relate to cybercrime.
Critique and evaluate key security vulnerabilities of data storage infrastructure.
Demonstrate a comprehensive understanding of threats to computer networks and physical infrastructure.

Demonstrate a comprehensive understanding of the key procedures and practices relevant to the management of cyber security risks and countermeasures.
Integrate and analyse relevant theoretical and case-based literature to present a sustained, coherent and logical consideration to cybercrime and cyber security

Assessment Tasks

Name	Weighting	Hurdle	Due
Tutorial Participation	10%	No	Ongoing
Weekly Quizzes	20%	No	Ongoing
Seminal Article Critique	20%	No	Week 7
Major Essay	50%	No	Week 11

Tutorial Participation

Due: **Ongoing**
Weighting: **10%**

See iLearn for additional information.

On successful completion you will be able to:

- Demonstrate a comprehensive understanding of the key crime types and criminological issues which relate to cybercrime.
- Critique and evaluate key security vulnerabilities of data storage infrastructure.
- Demonstrate a comprehensive understanding of threats to computer networks and physical infrastructure.
- Demonstrate a comprehensive understanding of the key procedures and practices relevant to the management of cyber security risks and countermeasures.
- Integrate and analyse relevant theoretical and case-based literature to present a sustained, coherent and logical consideration to cybercrime and cyber security

Weekly Quizzes

Due: **Ongoing**
Weighting: **20%**

Multiple choice weekly quizzes based on the readings and lectures from the week.

On successful completion you will be able to:

- Demonstrate a comprehensive understanding of the key crime types and criminological issues which relate to cybercrime.
- Critique and evaluate key security vulnerabilities of data storage infrastructure.

Seminal Article Critique

Due: **Week 7**
Weighting: **20%**

See iLearn for additional information.

On successful completion you will be able to:

- Demonstrate a comprehensive understanding of the key crime types and criminological issues which relate to cybercrime.
- Critique and evaluate key security vulnerabilities of data storage infrastructure.
- Demonstrate a comprehensive understanding of threats to computer networks and physical infrastructure.
- Demonstrate a comprehensive understanding of the key procedures and practices relevant to the management of cyber security risks and countermeasures.

Major Essay

Due: **Week 11**
Weighting: **50%**

See iLearn for additional information.

On successful completion you will be able to:

- Demonstrate a comprehensive understanding of the key crime types and criminological issues which relate to cybercrime.
- Critique and evaluate key security vulnerabilities of data storage infrastructure.
- Demonstrate a comprehensive understanding of threats to computer networks and physical infrastructure.
- Demonstrate a comprehensive understanding of the key procedures and practices relevant to the management of cyber security risks and countermeasures.
- Integrate and analyse relevant theoretical and case-based literature to present a sustained, coherent and logical consideration to cybercrime and cyber security

Delivery and Resources

UNIT REQUIREMENTS AND EXPECTATIONS

- You should spend an average of 12 hours per week on this unit. This includes listening to lectures prior to seminar or tutorial, reading weekly required materials as detailed in iLearn, participating in Ilearn discussion forums and preparing assessments.
- Internal students are expected to attend all seminar or tutorial sessions, and external students are expected to make significant contributions to on-line activities.
- In most cases students are required to attempt and submit all major assessment tasks in order to pass the unit.

REQUIRED READINGS

- The citations for all the required readings for this unit are available to enrolled students through the unit iLearn site, and at Macquarie University's library site. Electronic copies of required readings may be accessed through the library or will be made available by other means.

TECHNOLOGY USED AND REQUIRED

- Computer and internet access are essential for this unit. Basic computer skills and skills in word processing are also a requirement.
- This unit has an online presence. Login is via: https://ilearn.mq.edu.au/
- Students are required to have regular access to a computer and the internet. Mobile devices alone are not sufficient.
- Information about IT used at Macquarie University is available at http://students.mq.edu.au/it_services/

SUBMITTING ASSESSMENT TASKS

- All text-based assessment tasks are to be submitted, marked and returned electronically. This will only happen through the unit iLearn site.
- Assessment tasks must be submitted as a MS word document by the due date.
- Most assessment tasks will be subject to a 'TurnitIn' review as an automatic part of the submission process.
- The granting of extensions is subject to the university's Special Consideration Policy. Extensions will not be granted by unit conveners or tutors, but must be lodged through Special Consideration: https://students.mq.edu.au/study/my-study-program/special-consideration

LATE SUBMISSION OF ASSESSMENT TASKS

Unless a Special Consideration request has been submitted and approved, (a) **a penalty for lateness will apply** – two (2) marks out of 100 will be deducted per day for assignments submitted after the due date – and (b) **no assignment will be accepted seven (7) days (incl. weekends) after the original submission deadline**. No late submissions will be accepted for timed assessments – e.g. quizzes, online tests.

WORD LIMITS FOR ASSESSMENT TASKS

- Stated word limits include footnotes and footnoted references, but not bibliography, or title page.
- Word limits can generally deviate by 10% either over or under the stated figure.
- If the number of words exceeds the limit by more than 10%, then penalties will apply. These penalties are 2% of the total mark for every 100 words over the word limit. If a paper is 300 words over, for instance, it will lose 3 x 3% = 9% of the total mark assignment.
- The application of this penalty is at the discretion of the course convener.

REASSESSMENT OF ASSIGNMENTS DURING THE SEMESTER

- Macquarie University operates a Grade Appeal Policy in cases where students feel their work was graded inappropriately: http://www.mq.edu.au/policy/docs/gradeappeal/policy.html
- In accordance with the Grade Appeal Policy, individual works are not subject to regrading.

STAFF AVAILABILITY

- Department staff will endeavour to answer student enquiries in a timely manner. However, emails or iLearn messages will not usually be answered over the weekend or public holiday period.
- Students are encouraged to read the Unit Guide and look at instructions posted on the iLearn site before sending email requests to staff.

Unit Schedule

Week 1 - Introduction to the unit

Week 2 - Mass Surveillance & Censorship

Week 3 - Cyber Hygiene & Security Posture

Week 4 - Security Policy

Week 5 - Phishing

Week 6 - Information Security & Risk Management

Week 7 - Law Enforcement in the cyber world

Study Break

Week 8 - Cyber Security Frameworks

Week 9 - Network security

Week 10 - Threat detection and response

Week 11 - Digital Forensics

Week 12 - Infrastructure protection

Week 13 - Unit wrap up/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.)*

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

Commitment to Continuous Learning

Our graduates will have enquiring minds and a literate curiosity which will lead them to pursue knowledge for its own sake. They will continue to pursue learning in their careers and as they participate in the world. They will be capable of reflecting on their experiences and relationships with others and the environment, learning from them, and growing - personally, professionally and socially.

This graduate capability is supported by:

Learning outcomes

- Demonstrate a comprehensive understanding of the key crime types and criminological issues which relate to cybercrime.
- Critique and evaluate key security vulnerabilities of data storage infrastructure.
- Demonstrate a comprehensive understanding of threats to computer networks and physical infrastructure.
- Demonstrate a comprehensive understanding of the key procedures and practices relevant to the management of cyber security risks and countermeasures.
- Integrate and analyse relevant theoretical and case-based literature to present a sustained, coherent and logical consideration to cybercrime and cyber security

Assessment tasks

- Tutorial Participation
- Weekly Quizzes
- Seminal Article Critique
- Major Essay

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

- Demonstrate a comprehensive understanding of the key crime types and criminological

issues which relate to cybercrime.
- Critique and evaluate key security vulnerabilities of data storage infrastructure.
- Demonstrate a comprehensive understanding of threats to computer networks and physical infrastructure.
- Demonstrate a comprehensive understanding of the key procedures and practices relevant to the management of cyber security risks and countermeasures.
- Integrate and analyse relevant theoretical and case-based literature to present a sustained, coherent and logical consideration to cybercrime and cyber security

Assessment tasks

- Tutorial Participation
- Weekly Quizzes
- Seminal Article Critique
- Major Essay

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

- Critique and evaluate key security vulnerabilities of data storage infrastructure.
- Demonstrate a comprehensive understanding of threats to computer networks and physical infrastructure.
- Demonstrate a comprehensive understanding of the key procedures and practices relevant to the management of cyber security risks and countermeasures.
- Integrate and analyse relevant theoretical and case-based literature to present a sustained, coherent and logical consideration to cybercrime and cyber security

Assessment tasks

- Tutorial Participation
- Weekly Quizzes
- Seminal Article Critique
- Major Essay

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

- Critique and evaluate key security vulnerabilities of data storage infrastructure.
- Demonstrate a comprehensive understanding of the key procedures and practices relevant to the management of cyber security risks and countermeasures.
- Integrate and analyse relevant theoretical and case-based literature to present a sustained, coherent and logical consideration to cybercrime and cyber security

Assessment tasks

- Tutorial Participation
- Weekly Quizzes
- Seminal Article Critique
- Major Essay

Effective Communication

We want to develop in our students the ability to communicate and convey their views in forms effective with different audiences. We want our graduates to take with them the capability to read, listen, question, gather and evaluate information resources in a variety of formats, assess, write clearly, speak effectively, and to use visual communication and communication technologies as appropriate.

This graduate capability is supported by:

Learning outcomes

- Critique and evaluate key security vulnerabilities of data storage infrastructure.
- Demonstrate a comprehensive understanding of threats to computer networks and physical infrastructure.
- Demonstrate a comprehensive understanding of the key procedures and practices relevant to the management of cyber security risks and countermeasures.
- Integrate and analyse relevant theoretical and case-based literature to present a sustained, coherent and logical consideration to cybercrime and cyber security

Assessment tasks

- Tutorial Participation
- Seminal Article Critique
- Major Essay

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

- Demonstrate a comprehensive understanding of the key crime types and criminological issues which relate to cybercrime.
- Critique and evaluate key security vulnerabilities of data storage infrastructure.

Assessment tasks

- Tutorial Participation
- Seminal Article Critique
- Major Essay

Changes from Previous Offering

- Weekly quizzes replace larger quizzes
- Late penalty changes
- Word limit penalties