PICX311

Cyber Security in Practice

S2 OUA 2017

Department of Security Studies and Criminology

Contents

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
Kevin Cleary
kevin.cleary@mq.edu.au

Lecturer
Angela Irwin
angela.irwin@mq.edu.au
Contact via +61 2 9850 1427
Y3A 240
By Appointment

Prerequisites
12 units including PICX111

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 PICX111 which looks at non-traditional security threats in the twenty-first century. All enrolment queries should be directed to Open Universities Australia (OUA): see www.open.edu.au

Important Academic Dates

Information about important academic dates including deadlines for withdrawing from units are available at https://www.open.edu.au/student-admin-and-support/key-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.

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

Assessment Tasks

Name	Weighting	Hurdle	Due
Participation/Engagement	10%	No	Weekly
Online Quizzes	15%	No	see unit iLearn site
Seminal Article Critique	25%	No	see unit iLearn site
Major Essay	50%	No	See unit iLearn site

Participation/Engagement

Due: **Weekly**
Weighting: **10%**

This Assessment Task relates to the following Learning Outcomes:

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

On successful completion you will be able to:

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

Online Quizzes

Due: **see unit iLearn site**
Weighting: **15%**

This Assessment Task relates to the following Learning Outcomes:

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

On successful completion you will be able to:

- Demonstrate a comprehensive understanding of the key crime types and criminological issues which relate to cybercrime.
- Demonstrate a comprehensive understanding of the key procedures and practices relevant to the management of cyber security risks and countermeasures.
- Demonstrate a comprehensive understanding of the key procedures and practices relevant to the management of cyber security risks and countermeasures.
- Demonstrate a comprehensive understanding of the key procedures and practices relevant to the management of cyber security risks and countermeasures.

- Demonstrate a comprehensive understanding of threats to computer networks and physical infrastructure.
- Critique and evaluate key security vulnerabilities of data storage infrastructure.

Seminal Article Critique

Due: **see unit iLearn site**
Weighting: **25%**

This Assessment Task relates to the following Learning Outcomes:

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

On successful completion you will be able to:

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

Major Essay

Due: **See unit iLearn site**
Weighting: **50%**

This Assessment Task relates to the following Learning Outcomes:

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

On successful completion you will be able to:

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

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, 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.

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 Disruptions Policy. Extensions will not in normal circumstances be granted by unit conveners or tutors, but must be lodged through wellbeing.

LATE SUBMISSION OF ASSESSMENT TASKS

- If an assignment is submitted late, 5% of the available mark will be deducted for each day (including weekends) the paper is late.
- For example, if a paper is worth 20 marks, 1 mark will be deducted from the grade given for each day that it is late (i.e. a student given 15/20 who submitted 4 days late will lose 4 marks = 11/20).
- The same principle applies if an extension is granted and the assignment is submitted later than the amended date.

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 5% of the awarded mark for every 100 words over the word limit. If a paper is 300 words over, for instance, it will lose 3 x 5% = 15% of the total mark awarded for the assignment. This percentage is taken off the total mark, i.e. if a paper was graded at a credit (65%) and was 300 words over, it would be reduced by 15 marks to a pass (50%).
- 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.

STAFF AVAILABILITY

- Department staff will endeavor 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

Module 1 - Introduction to the unit

Module 2 - Digital identities

Module 3 - Espionage

Module 4 - Hacking

Module 5 - Cyber warfare

Module 6 - Information security and risk management

Module 7 - Infrastructure protection

Module 8 - Network security

Module 9 - Threat detection and response

Module 10 - Social media

Module 11 - Policing cyberspace

Module 12 - Surveillance and national security

Module 13 - Unit wrap up/conclusion

Policies and Procedures

Late Submission - applies unless otherwise stated elsewhere in the unit guide

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 more than seven (7) days (incl. weekends) after the original submission deadline. No late submissions will be accepted for timed assessments – e.g. quizzes, online tests.

Extension Request

Special Consideration Policy and Procedure (https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policies/special-consideration)

The University recognises that students may experience events or conditions that adversely affect their academic performance. If you experience serious and unavoidable difficulties at exam time or when assessment tasks are due, you can consider applying for Special Consideration.

You need to show that the circumstances:

1. were serious, unexpected and unavoidable
2. were beyond your control
3. caused substantial disruption to your academic work
4. substantially interfered with your otherwise satisfactory fulfilment of the unit requirements
5. lasted at least three consecutive days or a total of 5 days within the teaching period and prevented completion of an assessment task scheduled for a specific date.

If you feel that your studies have been impacted submit an application as follows:

1. Visit Ask MQ and use your OneID to log in

2. Fill in your relevant details
3. Attach supporting documents by clicking 'Add a reply', click 'Browse' and navigating to the files you want to attach, then click 'Submit Form' to send your notification and supporting documents
4. Please keep copies of your original documents, as they may be requested in the future as part of the assessment process

Outcome

Once your submission is assessed, an appropriate outcome will be organised.

OUA Specific Policies and Procedures

Withdrawal from a unit after the census date

You can withdraw from your subjects prior to the census date (last day to withdraw). If you successfully withdraw before the census date, you won't need to apply for Special Circumstances. If you find yourself unable to withdraw from your subjects before the census date - you might be able to apply for Special Circumstances. If you're eligible, we can refund your fees and overturn your fail grade.

If you're studying Single Subjects using FEE-HELP or paying up front, you can apply online.

If you're studying a degree using HECS-HELP, you'll need to apply directly to Macquarie University.

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.

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

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

Creative and Innovative

Our graduates will also be capable of creative thinking and of creating knowledge. They will be imaginative and open to experience and capable of innovation at work and in the community. We want them to be engaged in applying their critical, creative thinking.

This graduate capability is supported by:

Learning outcomes

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

Assessment tasks

- Participation/Engagement
- Seminal Article Critique
- Major Essay

Capable of Professional and Personal Judgement and Initiative

We want our graduates to have emotional intelligence and sound interpersonal skills and to demonstrate discernment and common sense in their professional and personal judgement. They will exercise initiative as needed. They will be capable of risk assessment, and be able to handle ambiguity and complexity, enabling them to be adaptable in diverse and changing environments.

This graduate capability is supported by:

Learning outcomes

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

Assessment tasks

- Participation/Engagement

- Online Quizzes
- Seminal Article Critique
- Major Essay

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

Assessment tasks

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

Assessment tasks

- Participation/Engagement
- Online 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

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

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

Assessment tasks

- Participation/Engagement
- Online 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

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

Assessment tasks

- Participation/Engagement
- Online 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

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

Assessment tasks

- Participation/Engagement
- Online Quizzes
- 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:

Assessment task

- Participation/Engagement

Socially and Environmentally Active and Responsible

We want our graduates to be aware of and have respect for self and others; to be able to work with others as a leader and a team player; to have a sense of connectedness with others and country; and to have a sense of mutual obligation. Our graduates should be informed and active participants in moving society towards sustainability.

This graduate capability is supported by:

Learning outcomes

- Integrate and analyse relevant theoretical and case-based literature to present a sustained, coherent and logical consideration to cybercrime and cyber security.
- Critique and evaluate key security vulnerabilities of data storage infrastructure.

Assessment task

- Participation/Engagement