



PICT311

Cyber Security in Practice

S1 Day 2016

Dept of Policing, Intelligence & Counter-Terrorism

Contents

<u>General Information</u>	2
<u>Learning Outcomes</u>	2
<u>Assessment Tasks</u>	3
<u>Delivery and Resources</u>	4
<u>Unit Schedule</u>	7
<u>Policies and Procedures</u>	7
<u>Graduate Capabilities</u>	8
<u>Changes since First Published</u>	13

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

Angela Irwin

angela.irwin@mq.edu.au

Michael Cohen

michael.cohen@mq.edu.au

Credit points

3

Prerequisites

39cp

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 cyber security in practice 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 identifies 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.

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	Due
Participation/engagement	10%	See unit iLearn site
Online quizzes	15%	See unit iLearn site
Seminal article critique	25%	See unit iLearn site
Major essay	50%	See unit iLearn site

Participation/engagement

Due: **See unit iLearn site**

Weighting: **10%**

See unit iLearn site for details.

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

Online quizzes

Due: **See unit iLearn site**

Weighting: **15%**

See unit iLearn site for details.

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: **See unit iLearn site**

Weighting: **25%**

See unit iLearn site for details.

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: **See unit iLearn site**

Weighting: **50%**

See unit iLearn site for details.

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 at least 9 hours per week on this unit. This includes completing weekly activities and readings detailed in iLearn.
- Internal students are expected to attend all lectures and tutorials and external students are expected to contribute to weekly on-line discussions.
- Students are required to 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 EReserve site. Electronic copies of required readings may be accessed at the EReserve site.

TECHNOLOGY USED AND REQUIRED

- Personal PC 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.
- For technical support go to: http://mq.edu.au/about_us/offices_and_units/informatics/help
- For student quick guides on the use of iLearn go to: http://mq.edu.au/iLearn/student_info/guides.htm

SUBMITTING ASSESSMENT TASKS

- All assessment tasks are to be submitted, marked and returned electronically. This will only happen through the unit iLearn site.
- Assessment tasks must be submitted either as a PDF or MS word document by the due date.
- Assessment tasks will be subject to a 'Turnitin' review as an automatic part of the submission process.
- The granting of extensions of up to one week are at the discretion of the unit convener. Any requests for extensions must be made in writing before the due date for the submission of the assessment task. Extensions beyond one week are subject to the university's Disruptions Policy (http://www.mq.edu.au/policy/docs/disruption_studies/policy.html#purpose).

LATE SUBMISSION OF ASSESSMENT TASKS

- If an assignment is submitted late, 5% of the available mark will be deducted for the first day and 2% for each subsequent day (including weekends)
- 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 do not include references, 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.
- The application of this penalty is at the discretion of the unit convenor.

REASSESSMENT OF ASSIGNMENTS DURING THE SEMESTER

- Macquarie University operates a Grade Appeal Policy in cases where students feel their work was graded inappropriately (<http://mq.edu.au/policy/docs/gradeappeal/policy.html>). This process involves all assignments submitted for that unit being reassessed. However, in exceptional cases students may request that a single piece of work is reassessed. The Department process for the reassessment of assignments for marking during the semester is as follows:
 - You must consult with the unit convenor - A reassessment will only be granted if you have sought and received feedback about your performance on the assessment from the convenor.
 - Apply to PICT's Director of Learning and Teaching (or delegated authority) for a reassessment - no more than 7 days after the unit convenor or class tutor has returned the assessment to you. You must make a sound academic case referring to the marking rubric, which demonstrates that you have consulted the unit convenor and as a result of this there is evidence that either the marking criteria were not provided, or there is insufficient feedback to justify the mark given.
 - If appropriate, the Head of Department (or delegated authority) will organise the reassessment of work.
 - The mark determined after reassessment will be the final mark in that assessment task, and this mark can be lower than the original.

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

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

New Assessment Policy in effect from Session 2 2016 http://mq.edu.au/policy/docs/assessment/policy_2016.html. For more information visit http://students.mq.edu.au/events/2016/07/19/new_assessment_policy_in_place_from_session_2/

Assessment Policy prior to Session 2 2016 <http://mq.edu.au/policy/docs/assessment/policy.html>

Grading Policy prior to Session 2 2016 <http://mq.edu.au/policy/docs/grading/policy.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 http://www.mq.edu.au/policy/docs/disruption_studies/policy.html *The Disruption to Studies Policy is effective from March 3 2014 and replaces the Special Consideration Policy.*

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

- 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

- 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.
- 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.

Assessment tasks

- Participation/engagement
- 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 outcome

- Demonstrate a comprehensive understanding of the key procedures and practices relevant to the management of cyber security risks and countermeasures.

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

- 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.
- 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

- 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.
- 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

- Participation/engagement
- 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.
- 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

- Participation/engagement
- 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 outcome

- Critique and evaluate key security vulnerabilities of data storage infrastructure.

Assessment task

- Participation/engagement

Changes since First Published

Date	Description
11/01/2016	For approval by HoD.