COURSE OUTLINE

CRM310 Introduction to Cyber Crime

Course Coordinator: Dennis Desmond (ddesmond@usc.edu.au) **School:** School of Law and Society

2021 | Semester 1

Online — ONLINE 1 — You can do this course without coming onto campus.

Please go to the USC website for up to date information on the teaching sessions and campuses where this course is usually offered.

1. What is this course about?

1.1. Description

In this online course you will be introduced to the cyber environment in which the digital examiner operates. This course develops your professional knowledge, qualities of thinking and digital collaboration skills needed to prepare you for the following technical cyber security courses. You will learn about the NIST Cybersecurity Framework: Identify, Protect, Detect, Respond and Recover and how cyber criminals target individuals and businesses, unlawfully seizing data and identities. You will also identify the dark markets where stolen data, identities and Intellectual Property is traded and how international law enforcement agencies operate to locate and prosecute cyber criminals.

1.2. How will this course be delivered?

ACTIVITY	HOURS	BEGINNING WEEK	FREQUENCY
ONLINE 1			
Tutorial/Workshop – This online course will take between 10-12 hours per week and may have a combination of: webinar, peer to peer collaboration, asynchronous online materials and work, and synchronous lecturer and peer to peer zoom meetings. There is also an alternate 24 hour Zoom Kaffee Klatsch discussion room. This tutorial allows students to gather online and ask questions, catch up on missed materials, and seek assistance from other students and staff.	1hr	Week 1	13 times

1.3. Course Topics

This course covers the following topics:

1: The history of cybercrime.

2: The criminal enterprise.

3: Identifying attackers, defenders and victims.

4: Technical cyber attacks.

5: Malicious software.

6: Social engineering attacks.

7: Internet fraud and the threat to the corporate network.

8: The business of cybercrime and investigations.

9: Corporate espionage.

10: Investigating the cybercrime.

11: The law enforcement response.

12: The criminal economy and markets.

13: Cryptocurrencies and the future of cyber security.

2. What level is this course?

300 Level (Graduate)

Demonstrating coherence and breadth or depth of knowledge and skills. Independent application of knowledge and skills in unfamiliar contexts. Meeting professional requirements and AQF descriptors for the degree. May require pre-requisites where discipline specific introductory or developing knowledge or skills is necessary. Normally undertaken in the third or fourth full-time study year of an undergraduate program.

3. What is the unit value of this course?

12 units

4. How does this course contribute to my learning?

	COURSE LEARNING OUTCOMES	GRADUATE QUALITIES
	On successful completion of this course, you should be able to...	Completing these tasks successfully will contribute to you becoming...
1	Describe and explain in depth the digital cybersecurity environment from the attacker's and defender's perspective.	Knowledgeable
2	Work collaboratively in a digital environment to compare and contrast a range of cyber investigative methodologies and strategies.	Empowered
3	Identify and explain the range of technical and social engineering methodologies cybercriminals use to locate and attack victims.	Empowered
4	Reflect on human vulnerabilities exploited in cybercrime.	Creative and critical thinker
5	Identify and discuss the physical, social and societal costs to individuals and the community from cybercrime events.	Sustainability-focussed
6	Communicate the results of cyber investigations to a variety of technical and non-technical audiences.	Engaged

5. Am I eligible to enrol in this course?

Refer to the USC Glossary of terms for definitions of “pre-requisites, co-requisites and anti-requisites”.

5.1. Pre-requisites

Completion of 96 units

5.2. Co-requisites

Not applicable

5.3. Anti-requisites

Not applicable

5.4. Specific assumed prior knowledge and skills (where applicable)

Not applicable

6. How am I going to be assessed?

6.1. Grading Scale

Standard Grading (GRD)

High Distinction (HD), Distinction (DN), Credit (CR), Pass (PS), Fail (FL).

6.2. Details of early feedback on progress

Using marking rubrics, students will participate in continuous peer and self-assessment during tutorials

6.3. Assessment tasks

DELIVERY MODE	TASK NO.	ASSESSMENT PRODUCT	INDIVIDUAL OR GROUP	WEIGHTING %	WHAT IS THE DURATION / LENGTH?	WHEN SHOULD I SUBMIT?	WHERE SHOULD I SUBMIT IT?
All	1	Report	Individual	40%	1,500 words	Week 7	Online Assignment Submission with plagiarism check
All	2	Artefact - Creative, and Written Piece	Group	20%	2,000 words	Week 11	Online Assignment Submission with plagiarism check
All	3	Case Study	Individual	40%	1,500 words	Exam Period	Online Assignment Submission with plagiarism check

All - Assessment Task 1: Cyber-attack methodologies and victim profiles

GOAL:	You will be able to explain the different methods criminals use to obtain access to corporate and personal data through technical and social engineering attacks. This task will also enable you to reflect and discuss the human vulnerabilities exploited in cybercrime.
PRODUCT:	Report
FORMAT:	You will produce a 1,500-word assignment identifying a variety of technical and social engineering methodologies cybercriminals use to gain access to corporate and personal data.
CRITERIA:	

No.		Learning Outcome assessed
1	Description of digital cybersecurity environment.	
2	Description of technical attack methodologies.	
3	Compare and contrast a variety of social engineering attack methodologies.	
4	Reflection and discussion of the consequences to the individual, business and community at large.	
5	Critical reflection on the decision-making process of the victim .	
6	Assessment criteria are mapped to the course learning outcomes.	1 2 3 4 5 6

All - Assessment Task 2: Cyber-attack methodologies and victim profiles

GOAL:	The purpose of this task is to develop digital group collaboration skills through becoming familiar with recent examples of cybercriminal activity affecting the community and generating knowledge across a wide variety of attack methodologies and victim profiles.
PRODUCT:	Artefact - Creative, and Written Piece
FORMAT:	You will operate within a group and discuss examples of online criminal behaviour. Your group will locate evidence of recent examples of online criminal behaviour, identifying the methodologies used and consequences to the victims. Once online discussions have been completed, each student will individually prepare a 2,000-word written report identifying the technologies and their impact on individuals and society from the online examples identified. Your group will provide evidence of digital collaboration. The general format will be each member collects data each week, checks in and shares findings, discusses implications with their group members and the final product is a consolidation of the best negotiated examples with a rationale and evidence o digital collaboration.
CRITERIA:	

No.		Learning Outcome assessed
1	Compare and contrast cyber investigative methods.	
2	Explanation of the cyber security environment.	
3	Relevance of articles/tools and summaries.	
4	Explanation of cybercrime impact and consequences.	
5	Digital collaboration	

All - Assessment Task 3: Hidden effects of cybercrime

GOAL:	This case study was designed to prompt you to think critically about the hidden effects of cybercrime on victims and the community.
PRODUCT:	Case Study
FORMAT:	The product to be presented is equivalent to 1,500-word report on the assessed cyber security risks and control environment required to address these risks. This will be accompanied with a Business Case directed to the Directors of the organisation. The format is a structured Assessment and Business Case.
CRITERIA:	

No.		Learning Outcome assessed
1	Identification and discussion of the physical, psychological, financial and health effects of cybercrime on victims.	
2	Identification and discussion of the effects of cybercrime on families of victims and the community as a whole	
3	Identification and discussion of the resources available to victims of cybercrime.	
4	Professional communication.	

7. Directed study hours

A 12-unit course will have total of 150 learning hours which will include directed study hours (including online if required), self-directed learning and completion of assessable tasks. Directed study hours may vary by location. Student workload is calculated at 12.5 learning hours per one unit.

8. What resources do I need to undertake this course?

Please note: Course information, including specific information of recommended readings, learning activities, resources, weekly readings, etc. are available on the course Blackboard site– Please log in as soon as possible.

8.1. Prescribed text(s) or course reader

Please note that you need to have regular access to the resource(s) listed below. Resources may be required or recommended.

REQUIRED?	AUTHOR	YEAR	TITLE	PUBLISHER
Required	Jonathon Clough	2015	Principles of Cybercrime	Cambridge University Press

8.2. Specific requirements

This is an online course therefore access to a computer and the internet for 10-12 hours per week is essential.

9. How are risks managed in this course?

Health and safety risks for this course have been assessed as low. It is your responsibility to review course material, search online, discuss with lecturers and peers and understand the health and safety risks associated with your specific course of study and to familiarise yourself with the University's general health and safety principles by reviewing the online induction training for students, and following the instructions of the University staff.

10. What administrative information is relevant to this course?

10.1. Assessment: Academic Integrity

Academic integrity is the ethical standard of university participation. It ensures that students graduate as a result of proving they are competent in their discipline. This is integral in maintaining the value of academic qualifications. Each industry has expectations and standards of the skills and knowledge within that discipline and these are reflected in assessment.

Academic integrity means that you do not engage in any activity that is considered to be academic fraud; including plagiarism, collusion or outsourcing any part of any assessment item to any other person. You are expected to be honest and ethical by completing all work yourself and indicating in your work which ideas and information were developed by you and which were taken from others. You cannot provide your assessment work to others. You are also expected to provide evidence of wide and critical reading, usually by using appropriate academic references.

In order to minimise incidents of academic fraud, this course may require that some of its assessment tasks, when submitted to Blackboard, are electronically checked through SafeAssign. This software allows for text comparisons to be made between your submitted assessment item and all other work that SafeAssign has access to.

10.2. Assessment: Additional Requirements

Your eligibility for supplementary assessment in a course is dependent of the following conditions applying:

The final mark is in the percentage range 47% to 49.4%
The course is graded using the Standard Grading scale
You have not failed an assessment task in the course due to academic misconduct.

10.3. Assessment: Submission penalties

Late submission of assessment tasks may be penalised at the following maximum rate:
- 5% (of the assessment task's identified value) per day for the first two days from the date identified as the due date for the assessment task.
- 10% (of the assessment task's identified value) for the third day - 20% (of the assessment task's identified value) for the fourth day and subsequent days up to and including seven days from the date identified as the due date for the assessment task.
- A result of zero is awarded for an assessment task submitted after seven days from the date identified as the due date for the assessment task. Weekdays and weekends are included in the calculation of days late. To request an extension you must contact your course coordinator to negotiate an outcome.

10.4. Study help

For help with course-specific advice, for example what information to include in your assessment, you should first contact your tutor, then your course coordinator, if needed.

If you require additional assistance, the Learning Advisers are trained professionals who are ready to help you develop a wide range of academic skills. Visit the Learning Advisers web page for more information, or contact Student Central for further assistance: +61 7 5430 2890 or studentcentral@usc.edu.au.

10.5. Wellbeing Services

Student Wellbeing provide free and confidential counselling on a wide range of personal, academic, social and psychological matters, to foster positive mental health and wellbeing for your academic success.

To book a confidential appointment go to Student Hub, email studentwellbeing@usc.edu.au or call 07 5430 1226.

10.6. AccessAbility Services

Ability Advisers ensure equal access to all aspects of university life. If your studies are affected by a disability, learning disorder mental health issue, , injury or illness, or you are a primary carer for someone with a disability or who is considered frail and aged, AccessAbility Services can provide access to appropriate reasonable adjustments and practical advice about the support and facilities available to you throughout the University.

To book a confidential appointment go to Student Hub, email AccessAbility@usc.edu.au or call 07 5430 2890.

10.7. Links to relevant University policy and procedures

For more information on Academic Learning & Teaching categories including:

- Assessment: Courses and Coursework Programs
- Review of Assessment and Final Grades
- Supplementary Assessment
- Administration of Central Examinations
- Deferred Examinations
- Student Academic Misconduct
- Students with a Disability

Visit the USC website: http://www.usc.edu.au/explore/policies-and-procedures#academic-learning-and-teaching

10.8. General Enquiries

In person:

- **USC Sunshine Coast** - Student Central, Ground Floor, Building C, 90 Sippy Downs Drive, Sippy Downs
- **USC Moreton Bay** - Service Centre, Ground Floor, Foundation Building, Gympie Road, Petrie
- **USC SouthBank** - Student Central, Building A4 (SW1), 52 Merivale Street, South Brisbane
- **USC Gympie** - Student Central, 71 Cartwright Road, Gympie
- **USC Fraser Coast** - Student Central, Student Central, Building A, 161 Old Maryborough Rd, Hervey Bay
- **USC Caboolture** - Student Central, Level 1 Building J, Cnr Manley and Tallon Street, Caboolture

Tel: +61 7 5430 2890

Email: studentcentral@usc.edu.au