USC

Course Outline

Code: SEC601
Title: Introduction to Cyber Security

School: Science & Engineering
Teaching Session: Semester 1
Year: 2020
Course Coordinator: Dr Graeme Edwards
Course Moderator: Associate Professor Clive Harfield

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 cybersecurity operations. You will develop the professional knowledge, qualities of thinking and digital collaboration skills needed to prepare you for future technical cyber security courses. You will explore the NIST Cybersecurity Framework 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 are traded and how international law enforcement agencies operate to locate and prosecute cyber criminals.

1.2 Field trips, WIL placements or activities required by professional accreditation

Activity	Details
Nil	Not applicable

2. What level is this course?

600 level Specialised - Demonstrating a specialised body of knowledge and set of skills for professional practice or further learning. Advanced application of knowledge and skills in unfamiliar contexts.

3. What is the unit value of this course?

12 units

4. How does this course contribute to my learning?

Specific Learning Outcomes On successful completion of this course, you should be able to:	**Assessment tasks** You will be assessed on the learning outcomes in task/s:	**Graduate Qualities or Professional Standards mapping** Completing these tasks successfully will contribute to:
Analyse the digital cybersecurity environment from the attacker's and defender's perspectives.	2	Knowledgeable
Apply a range of cyber investigative methodologies to understand how a crime has occurred.	1	Empowered
Work in digital environment to produce auditable evidence of collaboration.	2	Engaged
Identify and explain the range of technical and social engineering threats impacting individuals and organisations	1, 2, 3	Knowledgeable
Identify and rationalise the human and technical vulnerabilities exploited in cybercrime to understand human reasoning and prevent further attacks.	1	Creative and Critical Thinker
Develop a business case informed by control management frameworks to manage key cyber security risks to an organisation.	3	Empowered
Communicate the results of cyber investigations to a variety of technical and non-technical audiences.	1,2,3	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 Enrolment restrictions

Enrolled in SC509 or BU708

5.2 Pre-requisites

Nil

5.3 Co-requisites

Nil

5.4 Anti-requisites

Nil

5.5 Specific assumed prior knowledge and skills (where applicable)

Nil

6. How am I going to be assessed?

6.1 Grading scale

Standard – 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

Task No.	Assessment Product	Individual or Group	Weighting %	What is the duration / length?	When should I submit?	Where should I submit it?
1	Report	Individual	30%	2,500 words	Week 7	Online Assignment Submission with Plagiarism check
2	Artefact - Creative, and Written Piece	Group	30%	2,000 words	Week 11	Online Assignment Submission with Plagiarism check
3	Case Study	Individual	40%	2,500 words	Week 14	Online Assignment Submission with Plagiarism check
			100%			

Assessment Task 1: Cybercrime methodology report

Goal:	The goal of this task is to identify and 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 2,500-word report identifying a variety of technical and social engineering methodologies cybercriminals use to gain access to corporate and personal data.
Criteria:	• Identification and explanation of a range of technical and social engineering methodologies • Identification and rationalisation of the human and technical vulnerabilities exploited in cybercrime. • Communication of investigation results

Assessment 2: Cyber-attack methodologies and victim profiles

Goal:	The purpose of this task is to become 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:	Your group will collect and collate artefacts throughout the course. Your team will locate evidence of online criminal behaviour identifying methodologies used and consequences to the victims. A 2,000-word overview of the portfolio is required identifying the technologies and their impact on individuals and society. Your group will also 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 team member and the final product is a consolidation of the best negotiated examples with a rationale and evidence of digital collaboration.
Criteria:	• Analysis of the digital cybersecurity environment • Identification and explanation of technical and social engineering methodologies • Evidence of digital collaboration • Communication of investigation results

Assessment Task 3: Application of Cyber Security Risk Management and Controls

Goal:	The goal of the task is to examine the cyber security risk environment and the controls needed to effectively mitigate risks in a manner that achieves organisational outcomes.
Product:	Case Study
Format:	The product to be presented is equivalent to a 2,500-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:	• Identification and explanation of a range of technical and social engineering threats, their likelihood and impact on the case study organisation • Application of control management framework • Development of a business case for senior management Communication of results

7. Directed study hours

The directed study hours listed here are a portion of the workload for this course. 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. Student workload is calculated at 12.5 learning hours per one unit.

Location:	Directed study hours for location:
Online	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.

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

This is an online course. Please note that 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 as they are required:

Author	Year	Title	Publisher
Principles of Cybercrime 2nd edition	2015	Jonathon Clough	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 as a student 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. It is also your responsibility to familiarise yourself with the University's general health and safety principles by reviewing the online Health Safety and Wellbeing training module 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

Eligibility for Supplementary Assessment

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

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

10.3 Assessment: Submission penalties

Late submission of assessment tasks will 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 and supply the required documentation to negotiate an outcome.

10.4 Study help

In the first instance, you should contact your tutor, then the Course Coordinator. Additional assistance is provided to all students through Academic Skills Advisers. To book an appointment or find a drop-in session go to Student Hub.

Contact Student Central for further assistance: +61 7 5430 2890 or studentcentral@usc.edu.au

10.5 Wellbeing Services

Student Wellbeing Support Staff are available to assist on a wide range of personal, academic, social and psychological matters to foster positive mental health and wellbeing for your success. Student Wellbeing is comprised of professionally qualified staff in counselling, health and disability Services.

Ability Advisers ensure equal access to all aspects of university life. If your studies are affected by a disability, mental health issue, learning disorder, injury or illness, or you are a primary carer for someone with a disability, AccessAbility Services can provide assistance, advocacy and reasonable academic adjustments.

To book an appointment with either service go to Student Hub, email studentwellbeing@usc.edu.au or accessability@usc.edu.au or call 07 5430 1226

10.6 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

10.7 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