UNSW Course Outline

ZEIT8017 Cyber Crime and Cyber Security - 2024

Published on the 19 Feb 2024

General Course Information

Course Code : ZEIT8017
Year : 2024
Term : Semester 1
Teaching Period : Z1
Is a multi-term course? : No
Faculty : UNSW Canberra
Academic Unit : School of Systems and Computing
Delivery Mode : Online
Delivery Format : Standard
Delivery Location : UNSW Canberra at ADFA
Campus : UNSW Canberra
Study Level : Postgraduate
Units of Credit : 6

Useful Links

Handbook Class Timetable

Course Details & Outcomes

Course Description

The Internet is revolutionising our society by driving economic growth and giving people new ways to connect and cooperate. Falling costs mean accessing the Internet will become cheaper and more accessible, allowing more people worldwide to use it, 'democratising' the use of technology and feeding the flow of innovation and productivity.

As with most changes, increasing our reliance on cyberspace brings new opportunities and threats. While the Internet fosters open markets and open societies, this can also make users more vulnerable to criminals, activists and state actors who want to harm us by compromising or damaging our critical data and systems.

A safe and secure online environment enhances trust and confidence and contributes to a stable and productive community. Information and communications technology is an integral part of our daily lives. Whether people have a computer at home, use online banking services or receive electricity supplies, the community's reliance on technology is increasing.

Government and business also take advantage of opportunities for economic development through increased use of information technology and a technology aware population with Internet connections locally and overseas.

The increasing use and dependence on technology significantly influences the domestic and international law enforcement operating environment. Crimes, for example, fraud, scams, and harassment, can be facilitated by using technology which brings unique challenges to old crimes. Activities that fall under this category are often referred to as high tech crime, computer crimes or cybercrimes. Technology-enabled crime encompasses: 1) Crimes committed directly against computers and computer systems, and 2) The use of technology to commit or facilitate the commission of traditional crimes.

This Masters level 6.0 UOC course is designed to provide students with an understanding of what cybercrime is, including capabilities, jurisdiction, sovereignty, state responsibility, various cyberattack.
and defence tools, consequences, occupation and neutrality. This unit will examine responses to the emerging threats posed by the multiple forms of cybercrime and consider the effectiveness of strategies used to combat them. Students will gather information and analyse and evaluate trends and issues of cybercrime in a systematic, creative and insightful way.

Course Aims

This course covers the threats to computer systems and the countermeasures that can be put in place to minimise these. It also gives an introduction to securing modern networks with a particular focus on TCP/IP based systems.

It covers a wide range of security issues and concepts from authentication and encryption through to network threats and password management. Students will examine computer security issues from the perspective of detecting threats and implementing secure computing environments and will develop an understanding of modern tools and techniques that can be deployed to secure a network.

Course Learning Outcomes

Course Learning Outcomes	Australian Computing Society (ACS)
CLO1 : Explain the cybercrime and cyber security perspectives and their impact.	• ACS4 : Monitoring, Review and Improvement
CLO2 : Discuss cybercrime laws and prevention strategies.	• ACS3 : Technological Resources for ICT Education
CLO3 : Critically evaluate the current legislation that impacts cybercrimes and law enforcement responses to this legislation.	• ACS2 : ICT Academic Leadership and Staffing
CLO4 : Understand the impact of cybercrime on society and the security measures to prevent them.	• ACS4 : Monitoring, Review and Improvement

Course Learning Outcomes	Assessment Item
CLO1 : Explain the cybercrime and cyber security perspectives and their impact.	• Assignment 1 • Assignment 2 • Assignment 3
CLO2 : Discuss cybercrime laws and prevention strategies.	• Assignment 1 • Assignment 2 • Assignment 3
CLO3 : Critically evaluate the current legislation that impacts cybercrimes and law enforcement responses to this legislation.	• Assignment 2 • Assignment 3
CLO4 : Understand the impact of cybercrime on society and the security measures to prevent them.	• Assignment 3

Learning and Teaching Technologies

Moodle - Learning Management System | Microsoft Teams

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates	Australian Computing Society (ACS)
Assignment 1 Assessment Format: Individual	30%	Start Date: Not Applicable Due Date: 18/03/2024 11:59 PM	• ACS1 : Institutional Commitment to ICT education • ACS2 : ICT Academic Leadership and Staffing
Assignment 2 Assessment Format: Individual	20%	Start Date: Not Applicable Due Date: 29/04/2024 11:59 PM	
Assignment 3 Assessment Format: Individual	50%	Start Date: Not Applicable Due Date: 31/05/2024 11:59 PM	• ACS1 : Institutional Commitment to ICT education • ACS2 : ICT Academic Leadership and Staffing • ACS3 : Technological Resources for ICT Education • ACS4 : Monitoring, Review and Improvement

Assessment Details

Assignment 1

Assessment Overview

This could range from the ever-evolving menace of ransomware attacks, which cripple organizations by encrypting critical data and demanding ransom for its release, to the insidious tactics of phishing scams that deceive individuals into divulging sensitive information. The essay should not only provide a thorough understanding of the chosen threat but also critically analyse its impact on various sectors, assess the effectiveness of current mitigation strategies, and propose innovative solutions or improvements. This task is designed to enhance research skills, foster critical thinking, and enable students to contribute meaningfully to the discourse on cybersecurity challenges and solutions in our increasingly digital world.

Course Learning Outcomes

- CLO1 : Explain the cybercrime and cyber security perspectives and their impact.
- CLO2 : Discuss cybercrime laws and prevention strategies.

Detailed Assessment Description

The essay will assess students' ability to research, analyse and explain knowledge gained from the study.

Assignment submission Turnitin type

Not Applicable

Assignment 2

Assessment Overview

For this assignment, students are required to select a notable cyber-attack and create a comprehensive PowerPoint presentation analysing various aspects of the incident. This includes the background of the targeted organization, the nature and execution of the attack, the immediate and long-term impacts, the response by the affected entity, and the wider implications for cybersecurity policies and practices. The presentation should not only recount the events but also critically evaluate the effectiveness of the response strategies employed and propose lessons that can be learned to bolster cyber resilience in similar contexts. This task aims to enhance not only the students' research and analytical skills but also their ability to convey complex information effectively through a compelling and informative presentation.

Course Learning Outcomes

- CLO1 : Explain the cybercrime and cyber security perspectives and their impact.
- CLO2 : Discuss cybercrime laws and prevention strategies.
- CLO3 : Critically evaluate the current legislation that impacts cybercrimes and law enforcement responses to this legislation.

Detailed Assessment Description

PowerPoint Presentation will assess students' knowledge gained during the initial study weeks. The powerpoint presentations will require deep research on a topic. Online readings from books and papers will be provided in MOODLE. This material, plus students additional search on the Internet, will provide essential preparation and background for this assignment.

Assignment submission Turnitin type

Not Applicable

Assignment 3

Assessment Overview

While the term cybersecurity is often invoked in many information technology and data management settings, its explicit definition and underpinning principles are rarely discussed. Provide an in-depth examination of the concept, including exploring its origin and historical application and reviewing its evolution over the past decades and adoption during the digital era. The construct's implications in the contemporary information technology environment will also need to be explicitly discussed, along with its underpinning best practices.

Course Learning Outcomes

- CLO1 : Explain the cybercrime and cyber security perspectives and their impact.
- CLO2 : Discuss cybercrime laws and prevention strategies.
- CLO3 : Critically evaluate the current legislation that impacts cybercrimes and law enforcement responses to this legislation.
- CLO4 : Understand the impact of cybercrime on society and the security measures to prevent them.

Detailed Assessment Description

The research paper will assess students' ability to research, analyse and explain knowledge gained from the study.

Assignment submission Turnitin type

Not Applicable

General Assessment Information

Grading Basis

Standard

Requirements to pass course

The three assessment items form the requirements to complete this subject. To pass this subject, students will need to achieve at least 50 marks out of a total 100 marks overall.

Course Schedule

Teaching Week/Module	Activity Type	Content
Week 1 : 26 February - 1 March	Module	Cybercrime: What, Who, How and Why
Week 2 : 4 March - 8 March	Module	Introduction to Cybersecurity
Week 3 : 11 March - 15 March	Module	Fundamentals of cybercrime and Cybersecurity
Week 4 : 18 March - 22 March	Module	The role of the cybercrime law
Week 5 : 25 March - 29 March	Module	Cybercrime Prevention Strategies
Week 6 : 1 April - 5 April	Other	Mid-Semester Break
Week 7 : 22 April - 26 April	Module	Implication and Impact of Cybercrime on Society
Week 8 : 29 April - 3 May	Module	Cyber Threat Intelligence
Week 9 : 6 May - 10 May	Module	Privacy and Data Protection
Week 10 : 13 May - 17 May	Module	Access Control
Week 11 : 20 May - 24 May	Module	Steganography
Week 12 : 27 May - 31 May	Other	Complete Final Assignment for Submission on 31/5/2023
Week 13 : 3 June - 7 June	Other	Revision and Course End

Attendance Requirements

Not Applicable - as no class attendance is required

Course Resources

Recommended Resources

There is no textbook that students need to obtain. A variety of resource materials will be made available. These will comprise of:

• Recommended papers and chapters from textbooks, Internet-based documents, and other sources. In general, this will be made available through the Moodle pages for this course.

Course Evaluation and Development

One of the key priorities in the 2025 Strategy for UNSW is a drive for academic excellence in education. One of the ways of determining how well UNSW is progressing towards this goal is by listening to our own students. Students will be asked to complete the myExperience survey towards the end of this course.

Students can also provide feedback during the semester via direct contact with the lecturer, the "On-going Student Feedback" link in Moodle. Student-Staff Liaison Committee meetings in schools, informal feedback conducted by staff, and focus groups. Student opinions really do make a difference. Refer to the Moodle site for this course to see how the feedback from previous students has contributed to the course development.

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
Lecturer	Francesco Schiliro		Canberra	☒ +612 6190 6137☒		No	Yes
Convenor	Siqi Ma		Sydney			No	No

Other Useful Information

Academic Information

Course Evaluation and Development

One of the key priorities in the 2025 Strategy for UNSW is a drive for academic excellence in education. One of the ways of determining how well UNSW is progressing towards this goal is by listening to our own students. Students will be asked to complete the myExperience survey towards the end of each course.

Students can also provide feedback during the semester via: direct contact with the lecturer, the "On-going Student Feedback" link in Moodle, Student-Staff Liaison Committee meetings in schools, informal feedback conducted by staff, and focus groups (where applicable). Student opinions really do make a difference. Refer to the Moodle site for your course to see how the feedback from previous students has contributed to the course development.

Important note: Students are reminded that any feedback provided should be constructive and professional and that they are bound by the Student Code of Conduct.

https://www.gs.unsw.edu.au/policy/documents/studentcodepolicy.pdf

Equitable Learning Services (ELS)

Students living with neurodivergent, physical and/or mental health conditions or caring for someone with these conditions may be eligible for support through the Equitible Learning Services team. Equitable Learning Services is a free and confidential service that provides practical support to ensure your mental or physical health conditions do not adversely affect your studies.

Our team of dedicated **Equitable Learning Facilitators** (ELFs) are here to assist you through this process. We offer a number of services to make your education at UNSW easier and more equitable.

Further information about ELS for currently enrolled students can be found at: https://www.student.unsw.edu.au/equitable-learning

Academic Honesty and Plagarism

UNSW has an ongoing commitment to fostering a culture of learning informed by academic integrity. All UNSW staff and students have a responsibility to adhere to this principle of academic integrity. All students are expected to adhere to UNSW's Student Code of Conduct. Find relevant information at: Student Code of Conduct (unsw.edu.au)

Plagiarism undermines academic integrity and is not tolerated at UNSW. It is defined as using the words or ideas of others and passing them off as your own, and can take many forms, from deliberate cheating to accidental copying from a source without acknowledgement.

For more information, please refer to the following:

https://student.unsw.edu.au/plagiarism

Submission of Assessment Tasks

Special Consideration

Special Consideration is the process for assessing and addressing the impact on students of short-term events, that are beyond the control of the student, and that affect performance in a specific assessment task or tasks.

Applications for Special Consideration will be accepted in the following circumstances only:

- Where academic work has been hampered to a substantial degree by illness or other cause;
- The circumstances are unexpected and beyond the student's control;
- The circumstances could not have reasonably been anticipated, avoided or guarded against by the student; and either:

(i) they occurred during a critical study period and was 3 consecutive days or more duration, or a total of 5 days within the critical study period; or

(ii) they prevented the ability to complete, attend or submit an assessment task for a specific date (e.g. final exam, in class test/quiz, in class presentation)

Applications for Special Consideration must be made as soon as practicable after the problem occurs and at the latest within three working days of the assessment or the period covered by the supporting documentation.

By sitting or submitting the assessment task the student is declaring that they are fit to do so and cannot later apply for Special Consideration (UNSW 'fit to sit or submit' requirement).

Sitting, accessing or submitting an assessment task on the scheduled assessment date, after applying for special consideration, renders the special consideration application void.

Find more information about special consideration at: https://www.student.unsw.edu.au/special/

consideration/guide

Or apply for special consideration through your MyUNSW portal.

Late Submission of assessment tasks (other than examinations)

UNSW has a standard late submission penalty of:

- 5% per day,
- capped at five days (120 hours) from the assessment deadline, after which a student cannot submit an assessment, and
- no permitted variation.

Students are expected to manage their time to meet deadlines and to request extensions as early as possible before the deadline.

Electronic submission of assessment

Except where the nature of an assessment task precludes its electronic submission, all assessments must be submitted to an electronic repository, approved by UNSW or the Faculty, for archiving and subsequent marking and analysis.

Release of final mark

All marks obtained for assessment items during the session are provisional. The final mark as published by the university following the assessment review group meeting is the only official mark.

School-specific Information

The Leaning Management System

Moodle is the Learning Management System used at UNSW Canberra. All courses have a Moodle site which will become available to students at least one week before the start of semester. Please find all help and documentation (including Blackboard Collaborate) at the Moodle Support page.

UNSW Moodle supports the following web browsers:

• Google Chrome 50+

• Safari 10+

Internet Explorer is not recommended. Addons and Toolbars can affect any browser's performance.

Operating systems recommended are:
- Windows 10,
- Mac OSX Sierra,
- iPad IOS10

Further details:
Moodle System Requirements
Moodle Log In

If you need further assistance with Moodle:

For enrolment and login issues please contact:
IT Service Centre
Email: itservicecentre@unsw.edu.au
Phone: (02) 9385-1333
International: +61 2 9385 1333

For all other Moodle issues please contact:
External TELT Support
Email: externalteltsupport@unsw.edu.au
Phone: (02) 9385-3331
International: +61 2 938 53331
Opening hours:
Monday – Friday 7:30am – 9:30 pm
Saturday & Sunday 8:30 am – 4:30pm

Study at UNSW Canberra

Study at UNSW Canberra has lots of useful information regarding:
- Where to get help
- Administrative matters
- Getting your passwords set up
- How to log on to Moodle
- Accessing the Library and other areas.

UNSW Canberra Student Hub

For News and Notices, Student Services and Support, Campus Comminity, Quick Links, Important Dates and Upcoming Events

School Contact Information

Deputy Head of School (Education): Dr Erandi Hene Kankanamge
E: e.henekankanamge@adfa.edu.au
T: 02 5114 5157

Syscom Admin Support: syscom@unsw.edu.au
T: 02 5114 5284
Syscom Admin Office: Building 15, Level 1, Room 101 (open 10am to 3pm, Mon to Fri)