UNSW Course Outline

ZSPS9000 Foundations of Organisational Cyber Security - 2024

Published on the 29 Jan 2024

General Course Information

Course Code : ZSPS9000
Year : 2024
Term : Term 1
Teaching Period : T1
Is a multi-term course? : No
Faculty : UNSW Canberra
Academic Unit : Canberra School of Professional Studies
Delivery Mode : Online
Delivery Format : Standard
Delivery Location : Distance Education
Campus : Canberra City
Study Level : Postgraduate
Units of Credit : 6

Useful Links

Handbook Class Timetable

Course Details & Outcomes

Course Description

In order to be an effective leader, it is critical to have a solid understanding of the work others in

the discipline do. In cyber security, this means understanding a wide range of knowledge domains ranging from deeply technical fields through to legal and ethical considerations. Foundations of Organisational Cyber Security will focus on providing future leaders with a technical foundation to enrich their lexicon and enable effective communication with technical colleagues.

Course Aims

To create an understanding of a wide range of knowledge domains ranging from deeply technical fields through to legal and ethical considerations, whilst focusing on providing future leaders with a technical foundation to enrich their lexicon and enable effective communication with technical colleagues.

Course Learning Outcomes

Course Learning Outcomes
CLO1 : Describe the major principles and frameworks of cyber security.
CLO2 : Demonstrate a working knowledge of foundational technical concepts in cyber security.
CLO3 : Evaluate the impact of decisions made by cyber leaders across different organisational functions.
CLO4 : Analyse the interconnectedness between cyber security and broader organisational concepts.
CLO5 : Discuss the real-world applications, historical context and evolution of the discipline of cyber security.

Course Learning Outcomes	Assessment Item
CLO1 : Describe the major principles and frameworks of cyber security.	• Reflection on labs • Case study • Lessons Learned
CLO2 : Demonstrate a working knowledge of foundational technical concepts in cyber security.	• Reflection on labs • Case study • Lessons Learned
CLO3 : Evaluate the impact of decisions made by cyber leaders across different organisational functions.	• Reflection on labs • Case study • Lessons Learned
CLO4 : Analyse the interconnectedness between cyber security and broader organisational concepts.	• Case study • Lessons Learned
CLO5 : Discuss the real-world applications, historical context and evolution of the discipline of cyber security.	• Case study • Lessons Learned

Learning and Teaching Technologies

Moodle - Learning Management System | Zoom | Skillable

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates
Reflection on labs Assessment Format: Individual	30%	Start Date: Not Applicable Due Date: Week 10
Case study Assessment Format: Individual	30%	Start Date: Not Applicable Due Date: Week 5
Lessons Learned Assessment Format: Individual	40%	Start Date: Not Applicable Due Date: Week 12

Assessment Details

Reflection on labs

Assessment Overview

Lab exercises are focused on giving students hands-on experience with a cross-section of technical concepts. Students will be asked to reflect on the lab work in an organisational context.

Course Learning Outcomes

- CLO1 : Describe the major principles and frameworks of cyber security.
- CLO2 : Demonstrate a working knowledge of foundational technical concepts in cyber security.
- CLO3 : Evaluate the impact of decisions made by cyber leaders across different organisational functions.

Case study

Assessment Overview

Students will select a historical cyber incident and develop a case study that describes key features of the real-world event.

Course Learning Outcomes

- CLO1 : Describe the major principles and frameworks of cyber security.
- CLO2 : Demonstrate a working knowledge of foundational technical concepts in cyber security.
- CLO3 : Evaluate the impact of decisions made by cyber leaders across different organisational functions.

- CLO4 : Analyse the interconnectedness between cyber security and broader organisational concepts.
- CLO5 : Discuss the real-world applications, historical context and evolution of the discipline of cyber security.

Detailed Assessment Description

- This assessment has three deliverables before submission.
- In Week 2 you will be required to lock-in the cyber incident you will develop a case study on.
- In Week 4 you will be required present a draft version of your case study to your peers.
- You will be required to provide feedback to your peers on their presentations.

Lessons Learned

Assessment Overview

Students will select from a range of case studies focusing on a prior cyber incident. They will develop a lessons learned report, that focuses on the organisation at the centre of the selected case study - providing clear recommendations.

Course Learning Outcomes

- CLO1 : Describe the major principles and frameworks of cyber security.
- CLO2 : Demonstrate a working knowledge of foundational technical concepts in cyber security.
- CLO3 : Evaluate the impact of decisions made by cyber leaders across different organisational functions.
- CLO4 : Analyse the interconnectedness between cyber security and broader organisational concepts.
- CLO5 : Discuss the real-world applications, historical context and evolution of the discipline of cyber security.

General Assessment Information

Generative AI Statement:

UNSW accepts the potential of these tools and is excited to explore ways to use Generative AI (GenAI) to enrich your learning experience while maintaining the integrity of our programs and, therefore, of your degrees. We expect that, as we learn about how best to do this, our policies will adapt. For advice and guidance on how to use GenAI please see the Generative AI Statement in Moodle, or refer to the Universities resources: Chat GPT & Generative AI at UNSW | UNSW Current Students.

There are three key principles across the university:

1. Always do what you are asked to do in the assessment; if you don't follow the instructions, you

can't get marks.
2. If you are asked to do your own work, then that is what you should do, as we want to see that *you* have undertaken that learning rather than someone or something else.
3. When you incorporate ideas that are not your own, you should always acknowledge them. That applies in the world of AI, just as it did before.

In ***this course,*** the permitted level of GenAI use is '***Drafting Assistance***'.

What is Drafting Assistance?

As this course's assessment tasks involve some planning or creative processes, you are permitted to use software to generate initial drafts, ideas, structures, etc. However, you must develop or edit those ideas to such a significant extent that what is submitted is your own work, i.e., what is generated by the software should not be a part of your final submission. It is a good idea to keep copies of your initial drafts to show your lecturer if there is any uncertainty about the originality of your work.

Please note that your submission will be passed through an AI-text detection tool. If your marker has concerns that your answer contains passages of AI-generated text that have not been sufficiently modified, you may be asked to explain your work, but we recognise that you are permitted to use AI-generated text as a starting point, and some traces may remain. If you are unable to satisfactorily demonstrate your understanding of your submission, you may be referred to the UNSW Conduct & Integrity Office for investigation for academic misconduct and possible penalties.

Grading Basis

Standard

Requirements to pass course

In order to pass the course you must achieve an overall mark of at least 50%.

Course Schedule

Teaching Week/Module	Activity Type	Content
Week 1 : 12 February - 18 February	Online Activity	Introduction to Cyber
Week 2 : 19 February - 25 February	Online Activity	The History of Cyber
Week 3 : 26 February - 3 March	Online Activity	Technical Foundations
Week 4 : 4 March - 10 March	Online Activity	Cyber Risk
Week 5 : 11 March - 17 March	Online Activity	Threats, Vulnerabilities and Controls
Week 6 : 18 March - 24 March	Online Activity	The Cyber Environment and Industry
Week 7 : 25 March - 31 March	Online Activity	Cyber Ethics
Week 8 : 1 April - 7 April	Online Activity	Cyber in Organisations
Week 9 : 8 April - 14 April	Online Activity	Leadership and Decision-making
Week 10 : 15 April - 21 April	Online Activity	Key Cyber Challenges for Organisations

Attendance Requirements

Students are strongly encouraged to attend all classes and review lecture recordings.

Course Resources

Prescribed Resources

All resources required to complete this course are available via Moodle and Skillable (the Lab platform).

Recommended Resources

Student have access to a number of additional support resources.

Please check your Moodle page for additional readings and advice relevant to the course.

Course Evaluation and Development

Evaluation and Development

Toward the end of the hexamester you will be asked to give feedback about the course, via UNSW's MyExperience survey. Your feedback will be used, along with feedback from other stakeholders, to help improve the course. You can also contact your Course Convenor any time you have suggestions or other feedback.

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

Quality Assurance

UNSW actively monitors student learning and quality of the student experience in its programs. A random selection of completed assessment tasks may be used for quality assurance, such as determining the extent to which program learning goals are being achieved. The information is required for accreditation purposes, and aggregated findings will be used to inform changes aimed at improving the quality of programs. All material used for such processes will be treated as confidential.

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
Convenor	Tom Townsend					No	Yes

Other Useful Information

School-specific Information

ACADEMIC INFORMATION

Course Policies and Support

The Canberra School of Professional Studies expects students to be familiar with the contents of course outlines and UNSW's learning expectations, rules, policies and support services as listed below.

- Academic Integrity and Plagiarism
- Student Responsibilities and Conduct
- Special Consideration
- Cyber Security - Policies and Standards
- Cyber Security Policy
- Acceptable use of Information Resources Policy
- Use of AI for Assessments

Student Learning Outcomes

Course Learning Outcomes (CLOs) are competencies you should be able to demonstrate by the end of this course, if you participate fully in learning activities and successfully complete all assessment items.

CLOs contribute to the achievement of the Program Learning Outcomes (PLOs), which are developed across the duration of a program. PLOs are, in turn, directly linked to the UNSW graduate capabilities.

ACADEMIC HONESTY AND PLAGIARISM

As a student of UNSW you are expected to display academic integrity in your work interactions. Where a student breaches the UNSW Student Code with respect to academic integrity, the University may take disciplinary action under the Student Misconduct procedure. To assure academic integrity, you may be required to demonstrate reasoning, research and the process of constructing work submitted for assessment.

To assist you in understanding what academic integrity means, and how to ensure that you do comply with the UNSW Student Code, it is strongly recommended that you enrol in and complete the Working with Academic Integrity module before submitting your first assessment task. It is a free, online, self-paced Moodle module that should take no more than one hour to complete.

SUBMISSION OF ASSESSMENT TASKS

Special Consideration

Students can apply for special consideration when illness or other circumstances beyond your control interfere with your performance in a specific assessment task or tasks, including online exams.

Special consideration is primarily intended to provide you with an extra opportunity to demonstrate the level of performance of which you are capable. To apply, and for further information, see Special Consideration on the UNSW Current Students page.

Special considerations will be assessed centrally by the Case Review Team, who will update the online application with the outcome and add any relevant comments. The change to the status of the application immediately sends an email to the student and to the assessor with the outcome of the application.

Please note the following:

1. Applications can only be made through Online Services in myUNSW (see the UNSW Current Students page). Applications will not be accepted by teaching staff. The course convenor will

be automatically notified when your application is processed.
2. Applying for special consideration does not automatically mean that you will be granted a supplementary exam or other concession.
3. If you experience illness or misadventure in the lead up to an exam or assessment, you must submit an application for special consideration, either prior to the examination taking place or prior to the assessment submission deadline, except where illness or misadventure prevent you from doing so.
4. If your circumstances stop you from applying before your exam or assessment due date, you must apply within 3 working days of the assessment, or the period covered by your supporting documentation.
5. Under the UNSW Fit to Sit/Submit rule, if you sit the exam/submit an assignment, you are declaring yourself well enough to do so and cannot subsequently apply for special consideration.
6. If you become unwell on the day of - or during - an exam, you must stop working on your exam, advise your course convenor or tutor and provide a medical certificate dated within 24 hours of the exam, with your special consideration application. For online exams, you must contact your course convenor or tutor immediately via email, Moodle and advise them you are unwell and submit screenshots of your conversation along with your medical certificate and application.
7. Special consideration requests do not allow the awarding of additional marks to students.

Late Submission Penalties

For assessments other than examinations. late submission will normally incur a penalty of 5% per day or part thereof (including weekends) from the due date and time. An assessment will not be accepted after 5 days (120 hours) of the original deadline unless special consideration has been approved. An assignment is considered late if the requested format, such as hard copy or electronic copy, has not been submitted on time or where the 'wrong' assignment has been submitted.

For assessments which account for 10% or less of the overall course grade, and where answers are immediately discussed or debriefed, course convenor may stipulate a different penalty. Details of such late penalties will be available on the course Moodle page.

Feedback on Your Assessment Task Performance

Feedback on student performance from formative and summative assesment tasks will be provided to students in a timely manner. Assessment tasks completed within the teaching period of a course, other than the final assessment, will be assesed and students provided with feedback, with or without a provisional result, within 10 working days of submission, under normal circumstances. Feedback on continuous assessment tasks e.g., laboratory and studio-

based, workplace-based, weekly quizzes etc. will be provided prior to the mid-point of the course.

Protocol for Viewing Final Exams

1. Using their UNSW email address, students must lodge a request to view their final exam script within 3 working days immediately following the official release of overall course results.
   - This request must be lodged via email to CanberraSPS@canberra.unsw.edu.au with the subject line: **"REQUEST: View Exam Script"**.
   - In the body of the email, the student must provide their first name, zID, course code(s) and course name(s)
2. An email will be sent to the student with the viewing date and time, and location.
3. Exam script viewing will take place on campus and will be for a duration of no more than 30 minutes and will be under supervision of the lecturer or a nominated supervisor.
4. The student will need to present their zID credentials prior to being given access to the exam script.
5. At the designated viewing time, students must agree to NOT copy or photograph any part of any document or use recording software and/or devices to capture any aspect of the viewing or have access to any writing implement or any device capable of copying or photographing material e.g., mobile phones.
6. Wherever possible, students will be permitted to view their marked answers to multiple choice questions, but in exceptional circumstances this may not be possible.
7. There will be no opportunity to discuss or dispute the marks allocated for the final examination paper at this time.

Course Evaluation and Development

Feedback is regularly sought from students and continual improvements are based on this feedback. In week 9 of term, students are encouraged to complete a myExperience survey, which provides a key source of student evaluative feedback. Input into this quality enhancement process is extremely valuable in assisting us to meet the needs of our students and provide an effective and enriching learning experience. The results of all surveys are carefully considered and contribute towards enhancing educational quality.

Teaching Times and Locations

Please note that teaching times and locations are subject to change. Students are advised to refer to the Class Timetable website for the most up to date teaching times and locations.

School Contact Information

Academic enquiries

Email : canberrasps@canberra.unsw.edu.au

Phone: 02 5114 5369

Timetable, enrolment, wellbeing & health enquiries

Email : students@canberra.unsw.edu.au

Phone: 02 51145241