UNSW Course Outline

INFS5922 Contemporary Practices in Cybersecurity Management - 2024

Published on the 25 Aug 2024

General Course Information

Course Code : INFS5922
Year : 2024
Term : Term 3
Teaching Period : T3
Is a multi-term course? : No
Faculty : UNSW Business School
Academic Unit : School of Information Systems and Technology Management
Delivery Mode : In Person
Delivery Format : Standard
Delivery Location : Kensington
Campus : Sydney
Study Level : Postgraduate
Units of Credit : 6

Useful Links

Handbook Class Timetable

Course Details & Outcomes

Course Description

It is impossible to predict when cybersecurity incidents happen, but managers can decide how

prepared their business will be when they do. Beyond the technical aspects of cybersecurity, there are also many managerial and organisational issues that have to be addressed and carefully managed. These include internal and external communication, critical incident responses, and installing or refining a security framework with the appropriate controls to prevent future incidents. This course will cover the contemporary practices in cybersecurity management so that students are equipped with an understanding of how to manage and respond to these issues, as well as the short- to long-term implications of cybersecurity incidents.

Along with becoming familiar with concepts and frameworks that are grounded in data on actual attacks launched against businesses, students will learn how to formulate and prioritise measures that (1) prevent/reduce the impact of cybersecurity attacks, (2) prepare for an array of different attacks, and (3) enable the early detection of attacks. Students will also be exposed to methods for implementing automated controls in a cost-efficient and effective manner. This course is designed to facilitate the effective management of, and response to, a wide range of cybersecurity incidents, but the principles, practices, and recommendations covered may apply more broadly to a range of critical and adverse situations such as crises and natural disasters.

Course Aims

This course will equip students with the knowledge to lead or contribute to a cyber incident management team and help them to respond to cybersecurity incidents more quickly, efficiently and effectively. Students will also acquire knowledge on how to assess security and incident response frameworks, and design and implement automated controls to prevent or mitigate cybersecurity risks.

Course Learning Outcomes

Course Learning Outcomes	Program learning outcomes
CLO1 : Identify opportunities to enable cybersecurity controls through contemporary automation tools.	• PLO1 : Business Knowledge • PLO2 : Problem Solving • PLO3 : Business Communication • PLO5 : Responsible Business Practice
CLO2 : Assess the effectiveness of cybersecurity incidence response frameworks.	• PLO1 : Business Knowledge • PLO2 : Problem Solving • PLO3 : Business Communication
CLO3 : Formulate a plan to minimise the impact of cybersecurity incidents.	• PLO1 : Business Knowledge • PLO2 : Problem Solving • PLO3 : Business Communication • PLO4 : Teamwork • PLO5 : Responsible Business Practice
CLO4 : Demonstrate skills to communicate with a range of stakeholders.	• PLO1 : Business Knowledge • PLO3 : Business Communication • PLO4 : Teamwork
CLO5 : Demonstrate skills to work as part of an incident management team.	• PLO1 : Business Knowledge • PLO2 : Problem Solving • PLO3 : Business Communication • PLO4 : Teamwork

Course Learning Outcomes	Assessment Item
CLO1 : Identify opportunities to enable cybersecurity controls through contemporary automation tools.	• Invigilated Interview • Formative Workshops • Briefing to C-Suite Executives • Contract Pitch to Large Multinational
CLO2 : Assess the effectiveness of cybersecurity incidence response frameworks.	• Invigilated Interview • Formative Workshops • Briefing to C-Suite Executives • Contract Pitch to Large Multinational
CLO3 : Formulate a plan to minimise the impact of cybersecurity incidents.	• Invigilated Interview • Formative Workshops • Briefing to C-Suite Executives • Contract Pitch to Large Multinational
CLO4 : Demonstrate skills to communicate with a range of stakeholders.	• Invigilated Interview • Formative Workshops • Briefing to C-Suite Executives • Contract Pitch to Large Multinational
CLO5 : Demonstrate skills to work as part of an incident management team.	• Invigilated Interview • Formative Workshops • Contract Pitch to Large Multinational

Learning and Teaching Technologies

Moodle - Learning Management System

Learning and Teaching in this course

All readings and materials will be provided via Moodle.

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates	Program learning outcomes
Invigilated Interview Assessment Format: Individual	40%	Start Date: Not Applicable Due Date: Not Applicable	• PLO1 : Business Knowledge • PLO2 : Problem Solving • PLO5 : Responsible Business Practice
Formative Workshops Assessment Format: Individual	10%	Start Date: Not Applicable Due Date: Not Applicable	• PLO1 : Business Knowledge • PLO3 : Business Communication • PLO4 : Teamwork • PLO5 : Responsible Business Practice
Briefing to C-Suite Executives Assessment Format: Individual	20%	Start Date: Not Applicable Due Date: Not Applicable	• PLO1 : Business Knowledge • PLO3 : Business Communication • PLO5 : Responsible Business Practice
Contract Pitch to Large Multinational Assessment Format: Group	30%	Start Date: Not Applicable Due Date: Not Applicable	• PLO1 : Business Knowledge • PLO3 : Business Communication • PLO4 : Teamwork • PLO2 : Problem Solving

Assessment Details

Invigilated Interview

Assessment Overview

Final invigilated interview conducted during the exam period.

Course Learning Outcomes

- CLO1 : Identify opportunities to enable cybersecurity controls through contemporary automation tools.
- CLO2 : Assess the effectiveness of cybersecurity incidence response frameworks.
- CLO3 : Formulate a plan to minimise the impact of cybersecurity incidents.
- CLO4 : Demonstrate skills to communicate with a range of stakeholders.

- CLO5 : Demonstrate skills to work as part of an incident management team.

Detailed Assessment Description

This will take the form on an in-person oral interview. More information will be provided in class.

Assignment submission Turnitin type

Not Applicable

Generative AI Permission Level

Assistance with Attribution

This assessment requires you to write/create a first iteration of your submission yourself. You are then permitted to use generative AI tools, software or services to improve your submission in the ways set out below.
Any output of generative AI tools, software or services that is used within your assessment must be attributed with full referencing.
If outputs of generative AI tools, software or services form part of your submission and are not appropriately attributed, your Convenor will determine whether the omission is significant. If so, you may be asked to explain your submission. If you are unable to satisfactorily demonstrate your understanding of your submission you may be referred to UNSW Conduct & Integrity Office for investigation for academic misconduct and possible penalties.
For more information on Generative AI and permitted use please see here.

Formative Workshops

Assessment Overview

Regular workshop exercises that will be based around helping students develop the skills, knowledge and attitudes to engae with the content.

Course Learning Outcomes

- CLO1 : Identify opportunities to enable cybersecurity controls through contemporary automation tools.
- CLO2 : Assess the effectiveness of cybersecurity incidence response frameworks.
- CLO3 : Formulate a plan to minimise the impact of cybersecurity incidents.
- CLO4 : Demonstrate skills to communicate with a range of stakeholders.
- CLO5 : Demonstrate skills to work as part of an incident management team.

Detailed Assessment Description

You are expected to attended all the workshops and complete all in-class activities to get feedback from the teaching team.

Assignment submission Turnitin type

This is not a Turnitin assignment

Generative AI Permission Level

Assistance with Attribution

This assessment requires you to write/create a first iteration of your submission yourself. You are then permitted to use generative AI tools, software or services to improve your submission in the ways set out below.
Any output of generative AI tools, software or services that is used within your assessment must be attributed with full referencing.
If outputs of generative AI tools, software or services form part of your submission and are not appropriately attributed, your Convenor will determine whether the omission is significant. If so, you may be asked to explain your submission. If you are unable to satisfactorily demonstrate your understanding of your submission you may be referred to UNSW Conduct & Integrity Office for investigation for academic misconduct and possible penalties.
For more information on Generative AI and permitted use please see here.

Briefing to C-Suite Executives

Assessment Overview

Individual assessment to provide briefing to C-Suite Executives about cybersecurity.

Course Learning Outcomes

- CLO1 : Identify opportunities to enable cybersecurity controls through contemporary automation tools.
- CLO2 : Assess the effectiveness of cybersecurity incidence response frameworks.
- CLO3 : Formulate a plan to minimise the impact of cybersecurity incidents.
- CLO4 : Demonstrate skills to communicate with a range of stakeholders.

Detailed Assessment Description

This will take the form of a video. More information will be provided in class.

Assignment submission Turnitin type

Not Applicable

Generative AI Permission Level

Assistance with Attribution

This assessment requires you to write/create a first iteration of your submission yourself. You

are then permitted to use generative AI tools, software or services to improve your submission in the ways set out below.
Any output of generative AI tools, software or services that is used within your assessment must be attributed with full referencing.
If outputs of generative AI tools, software or services form part of your submission and are not appropriately attributed, your Convenor will determine whether the omission is significant. If so, you may be asked to explain your submission. If you are unable to satisfactorily demonstrate your understanding of your submission you may be referred to UNSW Conduct & Integrity Office for investigation for academic misconduct and possible penalties.
For more information on Generative AI and permitted use please see here.

Contract Pitch to Large Multinational

Assessment Overview

Contract Pitch to be undertaken by 3 to 4 students in a group for a Cybersecurity consulting project for a multinational.

Course Learning Outcomes

- CLO1 : Identify opportunities to enable cybersecurity controls through contemporary automation tools.
- CLO2 : Assess the effectiveness of cybersecurity incidence response frameworks.
- CLO3 : Formulate a plan to minimise the impact of cybersecurity incidents.
- CLO4 : Demonstrate skills to communicate with a range of stakeholders.
- CLO5 : Demonstrate skills to work as part of an incident management team.

Detailed Assessment Description

This will be a group video based on a scenario plus individual defence of the video presentation. More information will be provided in class.

Assignment submission Turnitin type

This is not a Turnitin assignment

Generative AI Permission Level

Assistance with Attribution

This assessment requires you to write/create a first iteration of your submission yourself. You are then permitted to use generative AI tools, software or services to improve your submission in the ways set out below.
Any output of generative AI tools, software or services that is used within your assessment must be attributed with full referencing.

If outputs of generative AI tools, software or services form part of your submission and are not appropriately attributed, your Convenor will determine whether the omission is significant. If so, you may be asked to explain your submission. If you are unable to satisfactorily demonstrate your understanding of your submission you may be referred to UNSW Conduct & Integrity Office for investigation for academic misconduct and possible penalties.
For more information on Generative AI and permitted use please see here.

General Assessment Information

Grading Basis

Standard

Course Schedule

Teaching Week/Module	Activity Type	Content
Week 0 : 2 September - 8 September	Activity	Read and become familiar with the course outline.
Week 1 : 9 September - 15 September	Workshop	Introduction & Course Admininistration Assessment introductions and expectations
Week 2 : 16 September - 22 September	Workshop	Threat Management
Week 3 : 23 September - 29 September	Workshop	Risk & Governanance
Week 4 : 30 September - 6 October	Workshop	Quantitative Risk Management
Week 5 : 7 October - 13 October	Workshop	Privacy Note: Week 5 Monday, 7 October 2024, is a public holiday. A pre-recorded lecture and workshop activities will be made available for Week 5.
Week 6 : 14 October - 20 October	Activity	Recharge Week Review course materials and work on your group project
Week 7 : 21 October - 27 October	Workshop	Cloud
Week 8 : 28 October - 3 November	Workshop	Secure Software Development
Week 9 : 4 November - 10 November	Workshop	Recent Trends, Operational Technology and Incident Response
Week 10 : 11 November - 17 November	Workshop	Group Assessments Preparations for Interviews

Attendance Requirements

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

Course Resources

Course Evaluation and Development

We will seek your feedback to improve this course via a mid-termsurvey and the end of term myExperience survey.

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
Lecturer	Pranit Anand		2076	9348 1398	Tuesday 10 to 11, Fridays 9 to 10	No	Yes

Other Useful Information

Academic Information

COURSE POLICIES AND SUPPORT

The Business School expects that you are familiar with the contents of this course outline and the UNSW and Business School learning expectations, rules, policies and support services as listed below:

- Program Learning Outcomes
- Academic Integrity and Plagiarism
- Student Responsibilities and Conduct
- Special Consideration
- Protocol for Viewing Final Exam Scripts
- Student Learning Support Services

Further information is provided on the Policies and Guidelines page.

Students may not circulate or post online any course materials such as handouts, exams, syllabi or similar resources from their courses without the written permission of their instructor.

STUDENT LEARNING OUTCOMES

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

CLOs also contribute to your achievement of the Program Learning Outcomes (PLOs), which are developed across the duration of a program. PLOs are, in turn, directly linked to UNSW graduate capabilities. More information on Coursework PLOs is available on the Policies and Guidelines page. For PG Research PLOs, including MPDBS, please refer to UNSW HDR learning outcomes.

Academic Honesty and Plagarism

As a student at UNSW you are expected to display academic integrity in your work and interactions. Where a student breaches the UNSW Code of Conduct with respect to academic integrity, the University may take disciplinary action. 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 Code of Conduct, it is strongly recommended that you 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 about one hour to complete.

Submission of Assessment Tasks

SHORT EXTENSIONS

Short Extension is a new process that allows you to apply for an extended deadline on your assessment without the need to provide supporting documentation, offering immediate approval during brief, life-disrupting events. Requests are automatically approved once submitted.

Short extensions are ONLY available for some assessments. Check your course outline or Moodle to see if this is offered for your assessments. Where a short extension exists, all students enrolled in that course in that term are eligible to apply. Further details are available the UNSW Current Students page.

SPECIAL CONSIDERATION

You 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.

Applications can only be made online and will NOT be accepted by teaching staff. Applications 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. The majority of applications will be processed within 3-5 working days.

For further information, and to apply, see Special Consideration on the UNSW Current Students page.

LATE SUBMISSION PENALTIES

LATE SUBMISSION PENALTIES

For assessments other than examinations, late submission will 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. In the case of an approved Equitable Learning Plan (ELP) provision, special consideration or short extension, the late penalty applies from the date of approved time extension. After five days from the extended deadline, the assessment cannot be submited.

An assessment is considered late if the requested format, such as hard copy or electronic copy, has not been submitted on time or where the 'wrong' assessment has been submitted.

For assessments which account for 10% or less of the overall course grade, and where answers are immediately discussed or debriefed, the LIC 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 assessment tasks will be provided to students in a timely manner. Assessment tasks completed within the teaching period of a course, other than a final assessment, will be assessed 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) will be provided prior to the midpoint of the course.

Faculty-specific Information

PROTOCOL FOR VIEWING FINAL EXAM SCRIPTS

UNSW students have the right to view their final exam scripts, subject to a small number of very specific exemptions. The UNSW Business School has set a protocol under which students may view their final exam script. Individual schools within the Faculty may also set up additional local processes for viewing final exam scripts, so it is important that you check with your School.

If you are completing courses from the following schools, please note the additional school-specific information:

- Students in the **School of Accounting, Auditing & Taxation** who wish to view their final examination script should also refer to this page.
- Students in the **School of Banking & Finance** should also refer to this page.
- Students in the **School of Information Systems & Technology Management** should also refer to this page.

COURSE EVALUATION AND DEVELOPMENT

Feedback is regularly sought from students and continual improvements are made based on this feedback. At the end of this course, you will be asked to complete the myExperience survey, which provides a key source of student evaluative feedback. Your 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 do lead to action towards enhancing educational quality.

QUALITY ASSURANCE

The Business School is actively monitoring student learning and quality of the student experience in all its programs. A random selection of completed assessment tasks may be used for quality assurance, such as to determine 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 Business School programs. All material used for such processes will be treated as confidential.

TEACHING TIMES AND LOCATIONS

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