UNSW Course Outline

ZZCA9222 Cyber Threats and Crime - 2024

Published on the 23 Apr 2024

General Course Information

Course Code : ZZCA9222
Year : 2024
Term : Hexamester 3
Teaching Period : KJ
Is a multi-term course? : No
Faculty : UNSW Canberra
Academic Unit : Canberra School of Professional Studies
Delivery Mode : Online
Delivery Format : Standard
Delivery Location : UNSW Canberra City
Campus : Canberra City
Study Level : Postgraduate
Units of Credit : 6

Useful Links

Handbook Class Timetable

Course Details & Outcomes

Course Description

The Internet drives economic growth and giving people new ways to connect and co-operate with one another. As with most change, increasing our reliance on cyberspace brings new opportunities but also new threats. While the internet fosters open markets and open societies,

this can also make users more vulnerable to criminals, activists, and foreign intelligence services who want to harm us by compromising or damaging our critical data and systems.

This course outlines, from a holistic perspective, the current and emerging trends in cybercrime and how they are being countered from an Australian perspective. It also discusses emerging technologies and how they might be misused.

Course Aims

This course equips students with the skills necessary to understand the current and evolving Australian cyber threat landscape. It outlines the historic and current aspects related to the field.

Course Learning Outcomes

Course Learning Outcomes
CLO1 : Identify and describe the different categories of both historical and contemporary computer crime.
CLO2 : Critically analyse the data and effect of online crime and the impact it has on government, businesses and individuals.
CLO3 : Critically evaluate the current legislation that impact on computer crimes and law enforcement and corporate responses to this legislation.
CLO4 : Explain the strengths and weaknesses of current controls to minimise the impact of cyber crime and terror.
CLO5 : Synthesise current trends to predict future trends in cyber crime and terror, and effectively communicate appropriate actions and controls.

Course Learning Outcomes	Assessment Item
CLO1 : Identify and describe the different categories of both historical and contemporary computer crime.	• Moodle discussion • Incident report • Final report
CLO2 : Critically analyse the data and effect of online crime and the impact it has on government, businesses and individuals.	• Moodle discussion • Incident report • Final report
CLO3 : Critically evaluate the current legislation that impact on computer crimes and law enforcement and corporate responses to this legislation.	• Post-incident review • Incident report • Final report
CLO4 : Explain the strengths and weaknesses of current controls to minimise the impact of cyber crime and terror.	• Post-incident review • Incident report • Final report
CLO5 : Synthesise current trends to predict future trends in cyber crime and terror, and effectively communicate appropriate actions and controls.	• Moodle discussion • Incident report • Final report

Learning and Teaching Technologies

Moodle - Learning Management System | Blackboard Collaborate

Learning and Teaching in this course

The Learning 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.

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

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates
Moodle discussion Assessment Format: Individual	10%	Due Date: Week 2
Incident report Assessment Format: Individual	25%	Due Date: Week 4
Post-incident review Assessment Format: Individual	25%	Due Date: Week 5
Final report Assessment Format: Individual	40%	Due Date: Week 7

Assessment Details

Moodle discussion

Assessment Overview

Write 500-words answering questions relating the course content and respond to another student's contribution.

Course Learning Outcomes

- CLO1 : Identify and describe the different categories of both historical and contemporary computer crime.
- CLO2 : Critically analyse the data and effect of online crime and the impact it has on government, businesses and individuals.
- CLO5 : Synthesise current trends to predict future trends in cyber crime and terror, and effectively communicate appropriate actions and controls.

Assessment Length

500 words

Incident report

Assessment Overview

Prepare a document suite in response to a hypothetical cyber incident in a workplace that would warrant internal escalation.

Course Learning Outcomes

- CLO1 : Identify and describe the different categories of both historical and contemporary computer crime.
- CLO2 : Critically analyse the data and effect of online crime and the impact it has on

government, businesses and individuals.
- CLO3 : Critically evaluate the current legislation that impact on computer crimes and law enforcement and corporate responses to this legislation.
- CLO4 : Explain the strengths and weaknesses of current controls to minimise the impact of cyber crime and terror.
- CLO5 : Synthesise current trends to predict future trends in cyber crime and terror, and effectively communicate appropriate actions and controls.

Assessment Length

1,750 words

Post-incident review

Assessment Overview

Building on the incident report, students will give a brief post-incident review as a presentation.

Course Learning Outcomes

- CLO3 : Critically evaluate the current legislation that impact on computer crimes and law enforcement and corporate responses to this legislation.
- CLO4 : Explain the strengths and weaknesses of current controls to minimise the impact of cyber crime and terror.

Assessment Length

5 minutes

Final report

Assessment Overview

Building on the incident report and post-incident review, students will produce a report that provide specific recommendations for the hypothetical organisation.

Course Learning Outcomes

- CLO1 : Identify and describe the different categories of both historical and contemporary computer crime.
- CLO2 : Critically analyse the data and effect of online crime and the impact it has on government, businesses and individuals.
- CLO3 : Critically evaluate the current legislation that impact on computer crimes and law enforcement and corporate responses to this legislation.
- CLO4 : Explain the strengths and weaknesses of current controls to minimise the impact of cyber crime and terror.
- CLO5 : Synthesise current trends to predict future trends in cyber crime and terror, and effectively communicate appropriate actions and controls.

Assessment Length

2,500 words

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.

Assessment Tolerances:

Assessment submissions have a tolerance of +/- 10% for length, meaning your submission length can go over or under the word or time limit by 10%. For example:

- A written assessment that has a 1,000-word limit can be between 900 and 1,100 words without penalty.
- An audio or video assessment that has a 10-minute time limit can be between 9 and 11 minutes without penalty.

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 : 6 May - 12 May	Online Activity	Cybercrime and threats in Australia & the Asia Pacific
Week 2 : 13 May - 19 May	Online Activity	Defending Australia - who's responsible?
Week 3 : 20 May - 26 May	Online Activity	Attacks
Week 4 : 27 May - 2 June	Online Activity	Protecting your data
Week 5 : 3 June - 9 June	Online Activity	Fraud
Week 6 : 10 June - 16 June	Online Activity	Ethics, warfare and foreign influence

Attendance Requirements

Not Applicable - as no class attendance is required

Course Resources

Prescribed Resources

All resources required to complete this course are available via Moodle.

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	Miranda Bruce					No	Yes
Postgraduate coordinator	Tom Townsend					No	No