INFO 2008 CYBER INCIDENT RESPONSE AND RISK MANAGEMENT

Credit Points 10

Coordinator Farhad Ahamed (https://directory.westernsydney.edu.au/search/name/Farhad Ahamed/)

Description Cyber risk management is the process of identifying, analysing, and evaluating how to handle an organisations' cyber security threats. This subject will introduce the fundamental tenets of risk management, and explore cybersecurity risk management frameworks. Cyber incident response is an organised approach to addressing and managing a major security breach, threat or attack. The goal is to handle the incident in a way that limits damage, reduces recovery time and losses, and take pro-active measures in the follow up and recovery phase to prevent future attacks. Students will explore common cyber attacks requiring incident response such as payment diversion fraud (business email compromise), ransomware, data breach, and advanced persistent threats. They will learn about each of these threats and how to manage such threats through the development of incident response plans including people, process, technology and information. This subject is taught with industry partners through case studies and simulations. Due to the sensitive nature of the subject and the requirement of hands on training, it cannot be taught online and is not on offer to WSU Online students. Online students will take an additional elective.

School Social Sciences

Discipline Security Science

Student Contribution Band HECS Band 2 10cp

Check your fees via the Fees (https://www.westernsydney.edu.au/currentstudents/current_students/fees/) page.

Level Undergraduate Level 2 subject

Co-requisite(s) COMP 2027 - Cyber Security

Restrictions

Students must be enrolled in course 1837 Bachelor of Cyber Security and Behaviour, or seek authorisation from the unit coordinator if they are studying another cybersecurity related program at Western Sydney University.

Learning Outcomes

1. Examine key concepts of risk management, common cyber risks, and cyber risk management frameworks.
2. Discuss fundamentals of cyber incident response.
3. Write an appropriate cyber incident response plan relevant to the organisation's needs.
4. Prepare for a cyber security incident through appropriate mechanisms.
5. Respond to cyber incidents through appropriate mechanisms.
6. Follow up post-incident using appropriate mechanisms.

Subject Content

- Risk Management
- Cyber Risks
- Cyber Risk Management Frameworks
- Cyber Incident Response
- Compliance and legal obligations when dealing with cyber incident

Assessment

The following table summarises the standard assessment tasks for this subject. Please note this is a guide only. Assessment tasks are regularly updated, where there is a difference your Learning Guide takes precedence.

Type	Length	Percent	Threshold	Individual/ Group Task
Quiz	10 X 10 MCQ each	10	N	Individual
Report	800 words	20	N	Individual
Simulation	24 hours	30	N	Group
Report	2000 words	40	N	Individual

Teaching Periods

Spring (2024)

Parramatta - Victoria Rd

On-site

Subject Contact Farhad Ahamed (https://directory.westernsydney.edu.au/search/name/Farhad Ahamed/)

View timetable (https://classregistration.westernsydney.edu.au/even/timetable/?subject_code=INFO2008_24-SPR_PS_1#subjects)