5.	Critically analyse different mitigation mechanisms and prevention to determining and evaluating possible security solutions.
6.	Critically analyse and describe different solutions for preventing cyber-attacks, and describe different network protection systems

Topics/Content outline:

Learning Outcome number and Time	Expanded Outcomes	Method	Assessment Type
1. (1 week)	Introduction to Cyber Space and IT Security Information Security: From device-centric to user-centric and modern security requirements • New trends and challenges of diverse platforms (Mobilization, BYOD, etc.) • Cloud, big data and virtualization • Application Security	Lecture Discussion, collaborative work, student presentations, critical reflection, on-line research, databases and industry inquiry.	Individual assignment
2. (1 week)	Network Security Technology • TCP/IP Concept • Understanding routers, firewalls and VPN • DMZ architecture • Firewall architecture • Deep packet inspection • Web application firewalls	Lecture Discussion, collaborative work, student presentations, (individual and collaborative exercises in the use of commercial tools and case studies)	Individual assignment
3. (1 week)	Three Phases of Cyber Attack Cycles • Preparation • Attack launch • Forensics	Lecture Discussion, collaborative work, critical reflection of on- line research, databases and industry inquiry.	Test: to review self-efficacy
4. (5 weeks)	Cyber Security and types of threats and hacking toolkits • Malicious Software • Viruses, worms & Trojans • Spywares and adwares	Lecture Discussion, collaborative work, student presentations, critical	Group and individual projects