RMIT UNIVERSITY

Master of Cyber Security

2019
Postgraduate

Secure data and fight cybercrime with the Master of Cyber Security. Learn to analyse and improve system and network security, assess and manage risk, and identify and diagnose cyberattacks.

Cyber security is a vital responsibility for organisations of all sizes, and in today's networked world it's more important than ever.

This program equips you with the mathematical, technical, analytical and business tools to protect and secure information systems from hacking threats and digital breaches.

You will learn the essentials of network and systems security, cybercrime and how to counter it with digital forensics, as well as risk analysis and management.

You will also learn about wired and wireless network security, cryptography, the Advanced Encryption Standard, RSA, smartcards, biometrics, ethical hacking, and information systems risk management.

This program includes opportunities for cyber security internships with industry organisations, both large and small.

Career outlook

Skilled graduates are required in a range of cyber security roles across all industries, as well as government and businesses of all sizes.

In an increasingly data-driven world, cyber security is a growing priority.

Global technology giant Cisco estimates that there are as many as one million vacant cyber security jobs around the world. Demand is expected to rise to six million jobs globally by 2019, with pay for cyber security professionals around 9 per cent higher than for other IT workers (Forbes, 2016).

Banking is an example of an industry investing heavily in cyber security experts to help protect them from hackers, but with so much personal data stored and shared in cyberspace everyday it's now a priority across the board.

Skilled graduates are highly sought after for cyber security roles, including:

- penetration testers
- IT risk analysts
- security managers
- forensic analysts
- security auditors
- network security engineers.

Learning and teaching

The program is offered through a flexible combination of lectures, tutorials and computer laboratory classes.

There are also opportunities for you to participate in team-based projects and to engage in consulting activities.

State-of-the-art cyber security software and work-simulated exercises are used in the program to provide you with hands-on experience.

Industry connections

In this program, you will complete specific courses that focus on work-integrated learning (WIL).

You will be assessed on your professional abilities in a workplace setting (real or simulated) and receive feedback from industry members.

Courses usually involve working on a real-world problem, where you will provide analysis, create a report and present your findings, receiving valuable feedback from industry partners.

You will also have an opportunity for an internship; previous students have interned with companies including Australia Post, Jemena, ANZ, and Victoria Police.

Program snapshot

Program code: MC159

Exit points

After completing 96 credit points of study approved by the program manager, you may exit with a graduate diploma.

Duration

Full-time: 2 years
Part-time: 4 years

Location

City campus

Program Coordinator

Associate Professor Serdar Boztas
Tel. +61 3 9925 2285
Email: smgs-infosec@rmit.edu.au

How to apply

Direct to RMIT University:
rmit.edu.au/programs/apply/direct

Fees

To learn how to calculate your fees visit:
rmit.edu.au/programs/fees/postgraduate

rmit.edu.au/programs/mc159

Program structure

The Master of Cyber Security consists of 192 credit points.

You will develop skills to apply a range of mathematical, analytical, algorithmic and computational techniques.

You will model and critically evaluate a range of cyber security systems and processes (hardware, software-based or a hybrid) that operate on a diverse range of media (optical, wireless or wired).

You will learn to use a variety of protocols (EFTPOS, INTERNET, CCITT) related to business or personal communications, keeping in mind the importance of ethical values in this service-oriented field.

There are four stages/semesters required to successfully complete the program.

Classes take a holistic approach to cyber security and are paired with insights from industry experts.

The program covers many topics, including risk management and cryptosystems, biometrics and ethical hacking.

Program elective examples

- Advanced Topics in Cryptography
- Algebra for Information Security
- Analysis of Large Data Sets
- Business Intelligence
- Cloud Security
- Coding of Cyber Communications
- Computer and Internet Forensics
- Data Communication and Net-Centric Computing
- Database Concepts
- Digital Innovation
- Digital Risk Management and Information Security
- Digital Strategy
- Ethical Hacking for Cyber Security
- Game Theory and its Applications
- Governance and Change in Digital Business
- Information Theory for Secure Communications
- Introduction to Statistical Computing
- Mathematical Modelling and Decision Analysis
- Secure Electronic Commerce
- Smartcards and Biometrics for Cyber Security.

Stage A	Case Studies in Cyber Security	Introduction to Information Security	Discrete Mathematics	Program elective
Stage B	Information Systems Risk Management	Program elective	Program elective	Program elective
Stage C	Cryptography for Cyber Security	Industry Awareness Project	Program elective	Program elective
Stage D	Industry Linkage Project	Program elective	Program elective	Program elective

Compulsory courses Program electives

Please note: This is an example of the program structure and program electives. Courses may change and may not be available each semester.

Credit and exemptions

You must have one of the following:

- An Australian bachelor degree with a minimum GPA of 2.0 out of 4.0 with award title including computer, IT, software, electrical, electronics, communications, mathematics, physics or equivalent

OR

- An Australian bachelor degree with a GPA between 1.5 and 2.0 out of 4.0 in a scientific/engineering/technical field with evidence of at least three years' work experience in the field of IT/information security or equivalent.

International qualifications are assessed according to the Australian Qualifications Framework (AQF).