Business Services
Chief Operating Officer Portfolio

Cybersecurity Advisory Manager

POSITION NUMBER 0061743

PROFESSIONAL CLASSIFICATION Senior Manager 1
STANDARD/SALARY An attractive remuneration package including superannuation

SUPERANNUATION Employer contribution of 11% or 17%

WORKING HOURS Full Time (1 FTE)

BASIS OF EMPLOYMENT Continuing

HOW TO APPLY Go to http://about.unimelb.edu.au/careers, under Current staff or Prospective staff, select the relevant option ('Current Opportunities' or 'Jobs available to current staff') and search for the position by title or number.

Name Tim Yeung
Tel +61 3 9035 4550
Email tim.yeung@unimelb.edu.au

Please do not send your application to this contact

For information about working for the University of Melbourne, visit our website: about.unimelb.edu.au/careers
ACKNOWLEDGEMENT OF COUNTRY

The University of Melbourne acknowledges the Traditional Owners of the unceded land on which we work, learn and live: the Wurundjeri Woi Wurrung and Bunurong peoples (Burnley, Fishermans Bend, Parkville, Southbank and Werribee campuses), the Yorta Yorta Nation (Dookie and Shepparton campuses), and the Dja Dja Wurrung people (Creswick campus).

The University also acknowledges and is grateful to the Traditional Owners, Elders and Knowledge Holders of all Indigenous nations and clans who have been instrumental in our reconciliation journey.

We recognise the unique place held by Aboriginal and Torres Strait Islander peoples as the original owners and custodians of the lands and waterways across the Australian continent, with histories of continuous connection dating back more than 60,000 years. We also acknowledge their enduring cultural practices of caring for Country.

We pay respect to Elders past, present and future, and acknowledge the importance of Indigenous knowledge in the Academy. As a community of researchers, teachers, professional staff and students we are privileged to work and learn every day with Indigenous colleagues and partners.

THE UNIVERSITY OF MELBOURNE

Established in 1853, the University of Melbourne is a leading international university with a tradition of excellence in teaching and research. The main campus in Parkville is recognised as the hub of Australia’s premier knowledge precinct comprising eight hospitals, many leading research institutes and a wide-range of knowledge-based industries. With outstanding performance in international rankings, the University is at the forefront of higher education in the Asia-Pacific region and the world.

The University of Melbourne employs people of outstanding calibre and offers a unique environment where staff are valued and rewarded.

Find out more about the University’s strategy, ‘Advancing Melbourne’, at https://about.unimelb.edu.au/strategy/advancing-melbourne

CHIEF OPERATING OFFICER PORTFOLIO

The Chief Operating Officer (COO) Portfolio enables quality outcomes for students, staff and partners by delivering University-wide services and operational support to meet the organisation’s evolving needs and strategic goals. The portfolio also works in partnership with teams across the University to drive innovation, transformation and improved performance, within and across functions. It is responsible for functions relating to the University’s finances, property, technology, legal and risk management, student and academic support, research and innovation services, operational performance, business services and sustainability.
The COO Portfolio is comprised of seven sub-portfolios:

- Business Services
- Chief Finance Officer Group
- Legal and Risk
- Office of the COO
- Operational Performance Group
- Research, Innovation and Commercialisation
- Student and Scholarly Services

**BUSINESS SERVICES**

Business Services provides a full range of class leading services to all operating entities of the University and comprises thirteen teams supporting the University community:

- Academic Technology: maintains and develops systems for research and student and learning.
- Campus Services: provides transport, cleaning, maintenance, security, and mail services.
- Client services: provides phone, in-person, and online services to the University.
- Cybersecurity: prevents, detects, and responds to threats, balancing risks with impacts.
- Enterprise Technology: maintains and develops the systems the University relies upon.
- Finance Operations: manages financial systems, obligations, and risk across the University.
- Health and Safety provide staff with access to knowledge and tools to work safely.
- HR Services: supports travel and payroll administration, recruitment, and development.
- Melbourne Bioresources: collaborates with researchers to maintain animal welfare standards.
- Program Delivery: leads the delivery of critical University capital programs.
- Research Computing services provides computing, data management and support services.
- Space Management: manages University spaces, tenancies, leases, and traders on campus.
- Strategy, Innovation, and Assurance provides IT strategy, innovation, and governance.

Business Services works with a shared set of values. These values give us simple cues to choose the

**EQUAL OPPORTUNITY, DIVERSITY, AND INCLUSION**

The University is an equal opportunity employer and is committed to providing a workplace free from all forms of unlawful discrimination, harassment, bullying, vilification and victimisation. The University makes decisions on employment, promotion, and reward on the basis of merit.

The University is committed to all aspects of equal opportunity, diversity and inclusion in the workplace and to providing all staff, students, contractors, honorary appointees, volunteers and visitors with a safe,
respectful and rewarding environment free from all forms of unlawful discrimination, harassment, vilification and victimisation. This commitment is set out in the Advancing Melbourne strategy that addresses diversity and inclusion, equal employment opportunity, discrimination, sexual harassment, bullying and appropriate workplace behaviour. All staff are required to comply with all University policies.

The University values diversity because we recognise that the differences in our people’s age, race, ethnicity, culture, gender, nationality, sexual orientation, physical ability and background bring richness to our work environment. Consequently, the People Strategy sets out the strategic aim to drive diversity and inclusion across the University to create an environment where the compounding benefits of a diverse workforce are recognised as vital in our continuous desire to strive for excellence and reach the targets of Advancing Melbourne.
ABOUT THE ROLE

Position Purpose:

The Cybersecurity Advisory Manager, under the guidance of the Associate Director of Cybersecurity Advisory, plays a leading role in directing our organization's cybersecurity efforts. Spearheading the provision of crucial insights to ongoing projects, this pivotal role ensures optimal cybersecurity outcomes through skilled consultant deployment. The Manager's commitment to aligning patterns with the University environment and eliminating legacy technologies drives innovative solutions. By embodying a proactive approach, they significantly enhance cybersecurity readiness and technological advancements for the institution.

Reporting line: Associate Director - Cybersecurity Advisory

Key Dimensions and Responsibilities:

No. of direct reports: 2
No. of indirect reports: 0
Direct budget accountability: N/A
Task level: Significant
Organisational knowledge: Significant
Judgement: Significant
Operational context: University wide

OH&S and compliance: All staff are required to take reasonable care for their own health and safety and that of other personnel who may be affected by their conduct. These include general staff responsibilities and those additional responsibilities that apply for managers, supervisors and other personnel. Specific responsibilities for the role are available at http://safety.unimelb.edu.au/topics/responsibilities/.

Staff must comply with all relevant requirements under the University’s risk management framework including legislation, statutes, regulations, and policies.
Core Accountabilities:

1. Provide strategic direction and leadership in the organization's cybersecurity efforts, working closely with the Associate Director of Cybersecurity Advisory to develop and execute a comprehensive cybersecurity strategy.
2. Lead and oversee ongoing cybersecurity engagements, ensuring this aligns with the organization's objectives and results in optimal cybersecurity outcomes.
3. Ensure cybersecurity advice and recommendations are aligned with the unique needs and environment of the University, taking into consideration academic and administrative requirements.
4. Identify and address legacy technologies and practices that may pose security risks, driving the adoption of innovative and up-to-date solutions to enhance cybersecurity.
5. Take a proactive stance in identifying potential security threats and vulnerabilities, developing and implementing preventive measures to enhance cybersecurity readiness.
6. Stay current with cybersecurity trends, emerging threats, and technological advancements, and integrate them into the organization's cybersecurity strategy and solutions.
7. Work closely with Cybersecurity Leadership team to support and deliver the long-term strategic roadmap for cybersecurity program

Selection Criteria:

1. Minimum of 8 years of relevant experience thereafter, or demonstrated extensive expertise and leadership in the field of Cybersecurity
2. Demonstrated ability to promote the values of Business Services:
   o University First, by always acting in the best interest of the broader University.
   o Service Excellence, by achieving high professional standards and taking ownership of service delivery.
   o One Team, by working adaptively and collaboratively, connecting with people, and building effective relationships across the workplace.
3. Well demonstrated expertise in cybersecurity principles, practices, and technologies, with a track record of successfully leading and advising on cybersecurity initiatives in a complex organizational setting.
4. Proven ability to lead and manage a team of cybersecurity consultants effectively, including hiring, mentoring, and fostering a collaborative and high-performing work environment.
5. Strong strategic thinking and planning skills, with the ability to develop and execute comprehensive cybersecurity strategies that align with the organization's goals and adapt to evolving threats.
6. Familiarity with the academic and administrative environment of a university or similar institution, including an understanding of the unique challenges and requirements associated with higher education.

7. A demonstrated track record of driving innovation in cybersecurity, including the ability to identify and eliminate legacy technologies and champion the adoption of cutting-edge solutions to enhance security posture.

8. Proven ability to proactively identify and mitigate cybersecurity risks and vulnerabilities, with a focus on preventive measures to enhance cybersecurity readiness.

9. Excellent communication and interpersonal skills, with the ability to effectively communicate complex cybersecurity concepts to a diverse range of stakeholders and build strong collaborative relationships across the organization.

**Other job-related information:**

Occasional work out of ordinary hours and occasional travel.