Position description

Position title	Cyber Security Analyst & Awareness Specialist
Position number	201163
Classification level	E
Group	Corporate Services
Reports to	Manager Enterprise Architecture & Security
Location	1010 La Trobe Street, Docklands 3008
Date	September 2024
Tenure	Permanent full time

Our organisation

VicTrack is custodial owner of Victoria's rail transport land, assets and infrastructure. We work to protect and grow the value of the portfolio, to support a thriving transport system and make travel and living better for all Victorians. With much of our asset portfolio dedicated to rail transport – our land, infrastructure, trams, trains and telecommunication networks – our focus is on strategic asset management and supporting the delivery of better transport solutions.

Whether we're planning and managing the use of transport land, upgrading the telecommunication network or partnering on major infrastructure projects, our job is to ensure the state's assets continue to serve Victoria now and well into the future.

Our core functions include:

- delivering telecommunications infrastructure and services that form the backbone of the transport network from signalling, driver communications, public information displays and myki ticketing
- managing land set aside for transport purposes, including the development and sale of land no longer required for transport to optimise its use
- generating income through land sales and commercial leases that is reinvested into the state's transport system
- providing project management, engineering and construction services to deliver a range of government transport projects from Victoria's Big Build to station and car park upgrades
- managing transport facilities and assets, including the open access Dynon Rail Freight Terminal, heritage buildings and environmental preservation.

VicTrack is the custodial owner of most of Victoria's tourist and heritage assets and performs the role of Tourist and Heritage Registrar.

Our business groups

Our business is made up of two specialist delivery groups – Property and Telecommunications – supported by Corporate Services, Strategy & Transformation and the Office of the Chief Executive.

Our vision

As a part of the transport portfolio, we share a common vision as defined in the *Transport Integration Act 2010*:

"To meet the aspirations of Victorians for an integrated and sustainable transport system that contributes to an inclusive, prosperous and environmentally responsible state".

In realising this vision, we are working towards
a transport system that promotes:

- social and economic inclusion
- economic prosperity
- environmental sustainability
- integration of transport and land use
- efficiency, coordination and reliability
- safety, health and wellbeing.

Our mission

To protect and grow our rail transport assets and drive reinvestment to service Victorians now and into the future.

Our values

- Professional – We make decisions with integrity and respect. By behaving professionally and ethically we win the trust of our colleagues, stakeholders and customers.
- Collaborate – We collaborate to get things done efficiently and effectively. We have greater opportunity through leveraging our collective knowledge, building stronger bonds and respecting each other.
- Achieve – We perform our roles with integrity and skill. We hold ourselves accountable for delivering what is needed and own both our successes and mistakes.
- Innovate – We embrace all new ideas that bring about change that adds value. We become more efficient, effective and competitive.

Dimensions

Reporting relationships

The Cyber Security Analyst & Awareness Specialist reports to the Manager Enterprise Architecture & Security in the Corporate Services Group.

Budget

N/A

Purpose of the position

The Cyber Security Analyst & Awareness Specialist is responsible for developing, implementing, and maintaining a comprehensive cyber security awareness program that educates and empowers employees at all levels. This position requires a proactive approach to identifying training needs and delivering engaging content that enhances our organisation's security culture.

The Specialist will also conduct various audit and assurance activities to assess the effectiveness of the cyber security controls and the levels of cyber security compliance.

Key accountabilities/functions

- Cyber security awareness and training, including:
  - Develop and implement a comprehensive cybersecurity awareness and training program tailored to various employee roles and third parties.
  - Create engaging and interactive training materials, including presentations, e-learning modules, videos, and quizzes.
  - Conduct regular training sessions, workshops, and webinars to educate employees on the latest cyber security threats, best practices, and company policies.
  - Collaborate with internal and external partners, such as IT, People & Culture, Change Manager, Communications team, and vendors, to coordinate and support the delivery of cyber security awareness and training initiatives.
  - Monitor and assess the effectiveness of the training program through feedback, surveys, and assessments.
  - Provide regular reports on training outcomes and identify areas for improvement.
  - Act as a cyber security advocate, promoting a culture of security awareness across the organisation.
  - Research and monitor emerging cyber security trends, threats, and best practices, and incorporate them into the awareness and training programs.
  - Support the creation of suitable awareness training to guarantee that the cyber security governance framework, policies and standards are effectively communicated throughout the organisation.
- Assurance: Audit, compliance and testing, including:
  - Lead and manage the Cyber Security Compliance Assurance program and schedule, the scope of which includes meeting cyber security related obligations, internal assessments, and facilitating audits and assurance of cyber security activities and objectives.
  - Lead and manage security testing exercises, ensuring the suitability of the IT disaster recovery plan and Cyber Security Incident Response plans.
  - Conduct control assurance testing of the information and cyber security controls in line with regulatory requirements and advise on corrective measures.
  - Prepare and present cyber security reports and dashboards to management and relevant stakeholders, providing insights and recommendations on cyber security testing findings and improvement opportunities.

Customer focus

VicTrack staff practise customer focus by recognising the importance of valuing customers (internal and external) and ensuring that all activities are oriented towards meeting customer needs. We listen to customers about their expectations and focus on delivering solutions that address their needs. Customer focus also includes proactively seeking and acting on feedback to enhance the customer experience.

Safety and environmental responsibilities

Ensure safety and environmental instructions are adhered to and report any inappropriate practices and incidents. Comply with the *Occupational Health and Safety Act,* as it applies to self, tenants and customers, and environmental legislation in regard to preserving the environment.

Rail safety

All staff who may be required to come into contact with rail activity, including design work and the management of other staff, must:

- be responsible for their actions where those actions can in any way affect or compromise railway safety
- be aware of the railway safety requirements associated with their duties and responsibilities
- take whatever action is possible to prevent unsafe conditions and/or incidents
- report any railway safety problems/hazards to the Manager Safety
- safely access the rail corridor.

Individual attributes

Qualifications

- A bachelor's degree or diploma in Information Technology (IT), computer science, software engineering, information systems, cyber security, data science or related technology field.

In addition to the above technical background, to be certified for this position, the incumbent must have one or more of the following industry-recognised Governance, Risk and Compliance certifications:

- Certified in Risk and Information Systems Control (CRISC) from ISACA (Information Systems Audit and Control Association)
- Certified Information System Security Professional (CISSP) from ISC2 (International Information System Security Certification Consortium)
- Certified Information Systems Auditor (CISA) from ISACA
- Certified in the Governance of Enterprise IT (CGEIT) from ISACA
- Certification in Risk Management Assurance (CRMA) from IIA (Institute of Internal Auditors)
- GRC Professional (GRCP) from OCEG (Open Compliance and Ethics Group)
- CompTIA Security+ from CompTIA
- Certified Ethical Hacker (CEH) certification from EC-Council
- Certified Information Security Manager (CISM) from ISACA
- Systems Security Certified Practitioner (SSCP) certification from ISC2

Knowledge and experience

- A minimum three years' experience working in a cyber security role, including cyber security training, awareness programs or similar governance, risk and compliance (GRC) role.
- Ability to work independently or as a collaborative team member, and inclusively build effective relationships and contribute towards a positive team environment.
- Working knowledge of cybersecurity principles, threats, and best practices including recognised Cyber Security Frameworks (e.g., VPDSF, NIST, ISM, Essential 8, ISO 27000 etc).
- Experience in the design, development and delivery of training and awareness materials utilising various tools and techniques including phishing simulation platforms.
- Experience with delivering cyber assurance activities across various security technologies, including technologies such as firewalls and network based cyber security controls, intrusion detection systems, anti-malware, EDR/XDR systems, web and cloud-based cyber security controls, modern identity security systems, log management, and content filtering.
- Experience in information security audit, assurance and compliance, identity and access management principles as well as coordinating penetration testing and vulnerability scans.

- Experience writing executive reports and dashboards.
- Knowledge of various IT domains, such as infrastructure, software, data, security, cloud, etc, obtained through previous technical hands-on roles or project experience.
- Experience and knowledge working in project teams under direction from project managers.

Skills

- Experience managing project stakeholders, including senior management, business users, IT staff, vendors, contractors, etc.
- Experience managing stakeholder communication, including developing and executing communication plans, preparing and delivering reports and presentations, and facilitating meetings and workshops.
- Experience preparing and presenting stakeholder education material, such as presentations, emails, phishing campaigns and cyber training courses.
- Experience and knowledge of using common e-learning, awareness and phishing simulation tools such as Proofpoint Awareness modules.
- Highly organised and able to prioritise conflicting deadlines and manage the expectations of others.
- A keen attention to detail and a commitment to quality and accuracy.

Interpersonal and other features

Internal relationships

- All VicTrack employees

External relationships

- Government departments and agencies
- All VicTrack customers
- Regulators
- Subcontractors
- Carriers and vendors