Job Description

27 February 25

Manager, Information Security SBS Technology

Reports to: Head of Technology Strategy and Architecture
Direct reports to this position: 4

SBS Values, Vision and Purpose

The Manager, Information Security is responsible for undertaking their work in a way that reflects SBS's Charter, Vision and Values and complies with relevant SBS policies, procedures and practices. At SBS, we expect you to be audience obsessed, be bold and brave, embrace difference, participate fully and ensure that we look out for one another. We are all working together to fulfil SBS's purpose and create a more cohesive society.

Division Purpose – Technology

SBS Technology can be thought of as the 'engine room' of SBS. Our primary role is to enable and support the production, distribution, and transmission of content across television, radio, and online platforms. Our teams achieve this by working collaboratively to design innovative solutions and deliver end-to-end services for our business stakeholders.

Role Purpose

The Manager, Information Security is responsible for overseeing the broader Cyber Security posture for SBS. This includes continuous development, execution and refinement of the Cyber Security strategy, establishment and operation of the technology capabilities protecting the organisation. Specifically, ensuring that SBS complies with industry regulations and frameworks e.g., ASD Essential 8, NIST and ISO27001 and managing internal / external audit and governance requirements.

The role directs staff in identifying, developing, implementing and maintaining processes across the business to minimise security risks as well as responding to incidents and establishing appropriate policies, standards, and controls. The role also oversees security operations for incident response and monitoring/addressing cyber incidents as well as security awareness training within the organisation.

Working with all parts of the business, it would provide you with deep insight into the inner workings of SBS and provide advice and guidance in security best practices. You will be a critical part of the Strategy and Architecture team, interacting closely with all parts of the technology team to support the needs of SBS.

Main Responsibilities

Main tasks of the role

Overview

- Managing the daily operation and implementation of the Technology security strategy
- Maintaining a current understanding the security threat landscape, compliance and regulatory obligations
- Creating, implementing and operating a strategy for the deployment of information security technologies, policies and practices
- Direct and approve the design of security systems
- Implement pro-active threat hunting and forensic investigation capabilities using available tools
- Draft review and approve security policies and controls and ensure communication to all personnel and that compliance is enforced
- Enhance cloud security strategies for AWS, Office 365 and EntraID, embedding security within CI/CD pipelines and cloud-native environments
- Brief the executive team on status and risks, including taking the role of champion for the overall strategy and budget requirements
- Oversee the third-party cyber risk program e.g., conducting vendor assessments to ensure compliance with SBS's security policies and regulatory expectations
- Management of security systems and applications, e.g., vulnerability management, identity and access management, endpoint protection, email protection
- Delivering new security technology approaches and implementing next generation solutions
- Manage and reporting of security KPI's and the tools e.g., ASD Essential 8 maturity, dwell time reduction, phishing simulation results and incident response effectiveness
- Lead the continuous enhancement of SBS's SIEM, ensuring optimal threat visibility, detection engineering and incident response capabilities
- Running security audits and risk assessments and ensuring all actions are complete in the agreed timeframes
- Oversee red team engagements and purple team exercises to continuously test and improve SBS's cyber resilience, moving towards and 'assumed breach' security model
- Cyber incident response planning and overseeing/performing investigation of reported security breaches
- Security awareness training to for all personnel and compliance enforcement
- Managing security employees and third parties involved in IT security
- Reporting to board/audit and risk committee on cyber security and managing associated risk treatment plans.
- Collaborate and provide Subject Matter Expertise to other SBS teams such as Privacy, Risk, Information Governance and Legal

Critical Incident Management

- Participate (escalation) as a Technical SME in the event of a critical cyber security incident to provide deeper knowledge and understanding
- Engage with SBS Third Party Cyber Security experts to co-ordinate additional support required during a critical cyber security incident

Leadership

- Ensure appropriate leadership, guidance and on-going technical subject matter expertise is provided to all stakeholders.
- Lead, motivate, and inspire a team of Cyber Security professionals, ensuring people are engaged, well managed and developed effectively to meet the current and future security needs of the

organisation. Provide coaching to support team members' growth and career development. Foster a positive and inclusive work environment where team members are encouraged to share ideas, enhance skills, and take ownership of security initiatives

Key relationships with other roles and external stakeholders

- Build and maintain a strong network of contacts and relationships across the Australian TV, digital media and technology vendor communities, both locally and internationally where appropriate.
- Represent the interests of SBS within appropriate forums and liaise with other stakeholders to ensure that the strategies and services reflect the operational needs and SBS Charter e.g., Privacy and Data Safety i.e., Information Governance, Legal, Risk, Privacy

Requirements of the role

Minimum requirements for the role

- Excellent communication skills across all levels of the organisation e.g., C-suite executives as well as technical resources and strong attention to detail
- Knowledge of ITIL Practices around Incident, Service Request, Problem and Change Management
- Experience in defining and enforcing security policies e.g., Password Standards, User Access Management, Acceptable Use of IT
- Monitor compliance with Information Security Policies, Standards and Procedures
- Deep understanding of security frameworks including ASD Essential 8, NIST, CSF, MITRE ATT&CK and ISO27001
- Solid foundations of IT fundamentals e.g., Web Applications, System Administration, networking
- Understanding of Architecture, Administration and OS
- Cloud security expertise with AWS, Microsoft O365 and EntraID (Azure AD) including IAM best practices and workload protection
- Experience with Intrusion Detection / Prevention Systems
- Experience with Security Information Event Management environments e.g., Elasticsearch, Splunk, Microsoft Sentinel
- Experience with Data Loss Protection
- Deep understanding of Risk Management Frameworks
- Deep understanding of Vulnerability Management
- Ability to define / refine processes for Network Security
- Ability to maintain security records of Monitoring and Incident Response activities
- Ability to perform analysis of security risks and develop mitigation strategies (including post-mortem deep forensics)
- Manage Cyber and Technical threat analyses e.g., Security monitoring, vulnerability management, penetration testing
- Ability to evaluate long-term technology solutions and vendors and articulate key design decisions and justifications
- Excellent analytical and problem-solving skills
- Managing self in a fast-paced environment with changing and competing priorities

- Understanding and appreciation of business drivers
- A strong customer and audience focus

Qualifications
- Bachelor or Master's degree in Information Technology / Computer Science or a related field
- Industry certification such as CISSP, CISM, GIAC, GCFA (Certified Forensic Analyst), OSCP (Offensive Security Certified Professional), AWS Security Specialty or Elastic Certified Engineer
- Extensive industry experience may be considered in lieu of formal qualifications

Desirable
- Experience in the broadcast and media industry
- Knowledge of security compliance requirements in Australian broadcast and media e.g., ACMA, OAIC
- Understanding of the lifecycle of media e.g., commissioning, acquisition, processing and distribution across TV, Radio and Online
- Understanding of video / audio systems including Media Asset Management systems e.g., Dalet, VizRT
- Understanding of digital media including Content Management Systems, streaming media formats and quality, Digital Rights Management and Content Delivery Networks
- Prior experience with leading and managing a small team of both technical and operational staff
- Project Management qualifications e.g., Prince2, PMP etc.
- Experience in Waterfall delivery – structured delivery frameworks
- Experience of Agile delivery including working with multiple end-to-end delivery streams

Key Capability		
Capability	**Level**	**Behaviour**
Coaching (People Leader Capability)	Organisation	• Creates links between coaching objectives and organisational strategies • Sets benchmark standards related to coaching practices • Role models above benchmark coaching values and behaviours • Gains organisational commitment to support a coaching culture • Encourages a high-performing coaching culture
Collaboration	Organisation	• Encourages collaboration (sharing of responsibility & information) across all levels of SBS • Promotes a climate of respect, helpfulness and co-operation across all levels of SBS • Encourages high-level stakeholders to work towards common business goals (i.e., across functions) • Sets the example for qualities such as respect, helpfulness and co-operation across the entire organisation

Customer Focus	Organisation	• Develops appropriate customer/client service strategies for SBS • Considers the impact of national/global trends in customer relationship management on SBS • Initiates the implementation of relevant customer/client service strategies • Ensures that principles of service are fostered throughout SBS
Innovation	Organisation	• Scans the environment for strategic opportunities to benefit SBS • Generates new ideas and innovative opportunities which move SBS forward • Is always thinking of the future positioning of SBS • Sponsors the development of creative business strategies • Promotes a culture that nurtures, recognises and rewards creativity & innovation
Organisational Awareness	Organisation	• Anticipates the impact of social, political & financial dynamics on SBS • Understands those social, political and financial dynamics that impact national/international markets & is up to date with competitors • Uses information regarding how functions work together to benefit the business • Promotes business sense & caution in the assessment of potential risks • Develops strong cost control measures • Uses financial reports when making organisational decisions
Results Focus	Organisation	• Strives to improve organisation and market performance • Ensures strategic initiatives are completed within designated timeframes • Fosters a culture that sustains excellence • Confronts obstacles in order to minimise their impact on organisational performance • Promotes the importance of meeting financial objectives across the business

Workplace Health & Safety

- Effectively promote and manage the work health and safety arrangements for the team as prescribed by the Health & Safety Management Arrangements.
    - Work Health & Safety Act (Cth) 2011
    - Work Health & Safety Act (Cth) Regulations 2011
    - WHS Hazardous Manual Tasks Code of Practice 2018
    - Work Health and Safety (How to Manage Work Health and Safety Risks) Code of Practice 2018
- Ensure employees are:
    - made aware of their WH&S responsibilities

- have received adequate safety induction and other WH&S information, instruction and training to enable them to conduct their work safely
- follow safe work practices

- Ensure the physical and psychological safety of the workplace under your control by:
  - ensuring regular workplace inspections are scheduled and conducted, involve the relevant HSR and recommendations made are actioned in a timely manner
  - ensuring compliance with the relevant standards and legislation in relation to purchase and provision of accommodation, furniture and equipment
  - identifying changes in the workplace/processes that may affect safety and ensuring that any associated risks are identified, assessed and controlled
  - verifying the effectiveness of control measures at appropriate intervals including monitoring compliance with safe operating procedures, site induction requirements and Permits to Work; and
- Ensure all WH&S reporting is accurately completed and submitted within specified timeframes and any follow up actions are completed
- Support/implement early intervention strategies and return to work programs.