Role Profile

Position Title	Head of Cyber Security
Reports To	Group CISO
FCA/PRA Approved Person Category(ies)	No
Date	April 2025

Job Summary

Riverstone International is a specialist insurer with its headquarters in the UK. The company is going through an exciting period following recent expansion with acquisitions in Ireland and the US and an expanded global footprint with offices in the UK (London, Brighton, Ipswich and Darlington) and internationally (Bermuda, USA, Ireland and Malta).

The Head of Cyber Security is responsible for leading the operational implementation of the organization's cyber security initiatives, ensuring robust protection against cyber threats, and managing key relationships. This role reports to the Group CISO and focuses on executing the cyber security strategy, optimizing the security architecture, managing vendor partnerships, overseeing software vulnerability management and other day-to-day security activities and strengthening collaboration with our Security Operations Centre (SOC) vendor partner.

We're looking for a hands-on leader who will manage our team of cyber security professionals, comprising two Cyber Security Associates based in London and an Information Security Officer. There will also be matrix influence of security-focussed colleagues in our Beverly, Massachusetts office. As such, the role holder is expected to be based in our London office at least three days per week.

Key Responsibilities and Competencies

Strategic Leadership:

- Oversee the operational implementation of the organization's cyber security architecture and supporting processes
- Work closely with the Group CISO and other senior leaders to align operational efforts with the organizational strategy
- Be a key member of the Group CISO senior leadership team
- Provide strategic direction and leadership to the cyber security team, ensuring alignment with business objectives, demonstrating a hands-on, servant leadership style in line with our "no egos" organisational value
- Work closely with the Data Governance & Security lead, who is responsible for the enhancement and maintenance of our policy and policy compliance framework, and the Head of IT.

Cyber security Operations:

- Evaluate the current cyber security toolset and make recommendations on new solutions to enhance security capabilities when appropriate
- Foster a strong and collaborative partnership with the organization's SOC provider, ensuring effective incident detection and response
- Build a strong collaborative relationship with the UK and US Heads of IT and provide challenge when required
- Monitor and respond to network and system security threats, such as unauthorized access and cyber-attacks
- Conduct regular security audits, identify vulnerabilities, and execute mitigation strategies
- Oversee the timely resolution of security-related findings from other teams (e.g. internal audit)
- Lead the operational response to security incidents and breaches, ensuring timely resolution and communication with relevant stakeholders

- **Vendor and Stakeholder Management**:
- Manage vendor relationships to ensure optimal service delivery and alignment with the organization's cyber security needs
- Engage with key stakeholders across the organization to promote cyber security awareness and best practices
- Key relationship owner with our SOC, forensics and incident response vendor partner

- **Innovation and Continuous Improvement**:
- Stay informed about cyber security trends, threats, and emerging technologies to adapt operational practices, making recommendations when needed
- Drive continuous improvement initiatives to enhance the organization's cyber security posture

- **Team Development**:
- Provide hands-on leadership and guidance to IT and cyber security teams
- Develop and mentor cyber security professionals, fostering a culture of excellence and continuous learning

Have an awareness of the Treating Customers Fairly ("TCF") and Conduct Risk strategies

On a temporary or permanent basis, you may be required to undertake other duties in addition to, or in substitution of, those listed in this role profile

Direct Reports

UK Cyber Security team (3 FTE) and matrix relationship with US-based colleagues

Internal Relationships

Group CISO, Group CIO, Regional CIOs

RiverStone International

Cyber Security Team Data Governance & Security Lead Head of IT IT Department (UK & Europe and US) Risk & Compliance Office of the CEO ExCo members

External Relationships

External partners, external consultants, suppliers

Authority to Act for the Company

None

Conduct Rules

The regulatory Conduct Rules set minimum standards of individual behaviour in financial services:

- You must act with integrity
- You must act with due care, skill and diligence
- You must be open and cooperative with the FCA, the PRA and other regulators
- You must pay due regard to the interests of customers and treat them fairly
- You must observe proper standards of market conduct where applicable
- All Conduct Rules staff to 'act to deliver good outcomes for retail customers' where the activities of the firm fall within the scope of the Duty

Conduct Standards

All employees are expected to abide by the RiverStone Code of Conduct

Competence – Experience

Qualifications and Skills:

- Bachelor's degree in Information Security, Computer Science, Engineering or a related discipline.
- Substantial experience in cyber security operations and leadership
- Certifications such as CISSP, CISM, or CEH are highly desirable
- In-depth understanding of cyber security frameworks and standards (e.g., NIST, ISO 27001)
- Strong problem-solving skills and the ability to manage complex, operational challenges
- Familiarity with UNIX scripting and tools such as Splunk is an advantage
- Excellent communication and collaboration skills to work effectively within teams and with senior leadership

Knowledge

Security Frameworks and Standards:

- Familiarity with industry-standard security frameworks such as ISO 27001, NIST, COBIT, and CIS Controls8. Understanding how to apply these frameworks to an organization's security strategy is crucial

Data Protection Laws and Regulations:

- Knowledge of global and regional data protection laws, such as GDPR, HIPAA, and CCPA, and how they impact data governance practices

Cyber security Technologies:

- Understanding of the technologies used to protect an organization's systems and data, including firewalls, intrusion detection systems, encryption, and access control mechanisms

Risk Assessment and Management:

- Ability to conduct risk assessments and implement risk management strategies to mitigate potential security threats

Data Governance Principles:

- Understanding of data governance frameworks and best practices for data quality, lifecycle management, and data architecture

Project Management:

- Proficiency in managing security and data governance projects, including budgeting, resource allocation, and timeline management

Communication and Training:

- Skills to effectively communicate security policies and train staff on security best practices and data handling procedures

Emerging Threats and Technologies:

- Continuous learning to stay abreast of emerging security threats and new technologies that can enhance security posture

Skills

- Excellent verbal and written communication skills with ability to communicate at all levels of the organisation
- Planning and implementation
- Project management
- Financial management
- Organisational skills
- Personal time management
- Strong interpersonal and collaborative skills
- Ability to establish relationships and influence key stakeholders at all levels
- Skills in policy development and stakeholder communication
- Expertise in data collaboration and fostering a culture of efficient data management

Confirmed as an accurate description of the role.

…… Date ……..
Role Holder

…… Date ……..
Manager