**Published Role Title**  
Head of Security Operations (SYS-33434)

**Type of Role**  
Perm

**Location**  
Street, Somerset

### Job Description

**Main Purpose:**  
The is to ensure that unauthorised access or damage to Clark’s computers, networks, programs and data is prevented. This position is a leadership role operating as part of Clark’s Cyber Security Leadership Team, requiring management of a matrix team spread across Clarks IT teams and 3rd party Cyber Security partners, and broad security domain knowledge across infrastructure, networks, Internet, www, applications and database environments. The Head of Cyber Security Operations is accountable for ensuring Clarks has appropriate and effective Cyber defences in place at all times and is fully prepared with effective cyber incident response plans.

**Core Accountabilities**

- **Cyber Security Operations**
  Own and manage the direct relationship with the Managed Security Services partner and other Security suppliers to ensure contractual commitments are delivered and drive continuous improvement.
  Define strategy for and lead the cyber security operations function to maintain the confidentiality, integrity and availability of Clarks systems and data
  Manage other IT teams in the provision of cyber security operations services
  Be responsible for undertaking security supplier relationship and commercial governance (supplier relationship roles, responsibilities and governance meetings) for the provision of security operations services
  Be responsible for ensuring that suppliers meet their contracted Cyber Security obligations
  Accountable for ensure contracted Security Services evolve to continually meet business needs
  Engagement across Group IT and Clarks to educate and motivate colleagues to be educated and aware of Cyber Security matters

- **Investigations and Incident Response**
  Lead Clarks’ response to major Cyber security incidents, coordinating response and managing communications with stakeholders up to Board level.
  Accountable for effectiveness of Security incident response activities, leading response teams with members from across the business.
  Ensure that Clarks has in place an effective Cyber Incident Response plan consisting of policies, processes and procedures that have been tested and communicated to all relevant parties across the organisation.
  Lead a team who will conduct formal investigations into inappropriate activity using Clarks computer systems
  Conduct regular analysis of Clarks’ Cyber Security incident and breach response performance and implement effective improvement programs.

**Key Outputs/Results**

- Implementation of 3rd party delivered Managed Security Services to budget and at pace, to give Clarks an effective ‘Detect & Respond’ capability to protect from Cyber-attack.
- Significant reduction in time to detect Cyber-attacks, resulting in reduction of potential impact to Clarks.
- Full suite of Cyber incident response playbooks developed to ensure all stakeholders are able to respond to Cyber incidents at pace and effectively.
- Effective cross-team virtual Incident Response teams able to respond to Cyber Attacks in line with developed playbooks.

**Resource Accountabilities**

- **Financial (Direct and indirect influence):**
  Direct accountability for circa £750k annual budget from 2020 onwards.
- **People (FTE – Direct and Indirect responsibility):**
  Direct line management of 1 Clarks employee and circa 10-15 from Managed Services Partner.

**Other Measures (e.g. Responsibility for Revenue/ Equipment/Property):**

**Key Relationships**

- Director of Technical Services and their direct reports
- Managed Security Services partner
- Data Privacy Officer
- Group Director of Risk & Internal Audit
- Regional HR Directors
- Law enforcement

**Essential Knowledge:**

- Relevant experience at a senior level in mid to large organisations.
- Deep knowledge and experience in:
Applications
Infrastructure Networks
Database Information Security
Identity and Access Management
Defence against Malware
Data leakage protection
Encryption.
Types of cyber-attack and their detection methods
Setting up / configuring security tools
Scoping penetration testing and producing corrective action plans to address breaches and vulnerabilities
Methods and motivations adopted by hackers to attack IT platforms and automated information systems
IT security incident management processes and tools
IT operations and support organizations
Understanding of applicable UK law and regulations in relation to IT Security
Experience taking a lead role in running security incidents and response teams.
Knowledge of ethical hacking and vulnerability research
Experience of running cyber security awareness initiatives
Previous experience analysis of security controls, identity, authentication & access controls
Security Event Monitoring
Vulnerability Management
Database Activity Monitoring
Privileged IT User Monitoring
Data Loss Prevention
Endpoint Security Controls
Email Security Controls
PCI DSS environment management
Two factor authentication solutions
IDS/IPS & Network Security
Developing corporate security architecture in response to changing threat landscape.
Developing departmental metrics and MI to validate BSI's IT security & control posture.
Management of 3rd party Cyber Security and IT Security assessments when required.

Technical Skills:
Disciplined work approach with the ability to co-ordinate multiple activities across a span of control of IT and business colleagues with high attention to detail
Clear written and verbal communication skills with the ability to clearly explain Cyber Security and IT Security issues and solutions to a non-technical audience
IT security forensic techniques, tools and procedures
Ability to work independently and collaboratively with business leaders, department heads and direct team
One or more formal Cyber Security and IT Security qualification from the following (e.g. MSc in Information Security, CISM, CISSP, GSNA, GCFA, GPEN, GSSP etc)
Proven negotiation and influencing skills
Expert influencing and negotiating skills
High attention to value for money.
Develop & maintain effective relationships with security partners and internal stakeholder groups including Internal Audit, Operational Risk and Information Security.

Successful Experience:
Experience of managing offshore-provided IT service, operations and support
Design, build, procurement and implementation of Security Operations Centres utilising Managed Security Services
Ability to meet targets and/or mitigate significant Cyber Security risks at pace
Significant experience in Cyber Security Incident response to large scale Cyber Attacks.