BritishRedCross

Cyber Security Team Manager

Job Level	5	**Korn Ferry Function**	KF 17
Directorate	Technology	**Function/Service**	Cyber Security
Direct Reports	6	**Indirect Reports**	None
Line Manager Title	Head of Cyber Security	**Budgetary Responsibility**	None

The Leadership and Management of our people is critical to us as an organisation. The responsibilities and expectations of Leaders and Managers at this level can be found in Our Leadership Framework - RedRoom.

Our Leadership Framework defines the leadership standards we want to see at the British Red Cross. It shows what great leadership looks like. Our goal is to create a great workplace and deliver excellent services to our users. Our Leadership Framework - RedRoom, along with Our values and behaviours - RedRoom and Fundamental Principles, helps everyone understand how the leadership capabilities relate to their role and context.

Diversity is something we celebrate, and we want you to be able to bring your authentic self to the British Red Cross. We want you to feel that you are in an inclusive environment, and a great position to help us spread the power of kindness. You can read more about Equity, Diversity & Inclusion (EDI) at the British Red Cross - RedRoom here.

Role Description	
Purpose	The role provides people leadership and delivery management for the British Red Cross Cyber Security Operations team, who are responsible for day-to-day security operations, including monitoring, threat detection, incident response, and vulnerability management. The role is a key interface between the operations team and stakeholders across the charity, supporting difficult conversations and acting as an escalation point to ensure that cyber security risks and issues are properly communicated, understood, and addressed in a timely manner. The role is accountable for ensuring that the team's workload is structured, prioritised, and delivered effectively to meet the needs of the organisation as well as fostering sustainable working practices.
Key Responsibilities	**Culture & Change** • Lead and manage the cyber security operations team to deliver effective security services across the organisation, including setting clear objectives and priorities across both reactive work, such as incident handling, and proactive initiatives, such as improvements and automation. • Cultivate a culture of continuous improvement within the team. • Monitor team capacity and skill sets, ensuring work is allocated to the right people and that workload is realistic and balanced. • Adjust resourcing, priorities, and plans in response to changing demand or urgent issues.

	• Support senior engineers in identifying and delivering improvements to security controls and processes. **Security Operations & Incident Handling** • Oversee day-to-day cyber security operations, ensuring controls and processes operate effectively across security monitoring, threat detection and response, vulnerability management, and secure configuration. • Act as the management escalation point for critical cyber incidents and security issues. • Help coordinate major incident response with the team and relevant incident management roles, ensuring timely resolution and clear stakeholder communication throughout. • Support structured post-incident reviews and blameless post-mortems to identify root causes and drive improvements. **Operating Model & Processes** • Implement and refine a clear operating model for the security operations function, aligned to best practice. • Develop and maintain playbooks, runbooks, and standard operating procedures to ensure consistent and efficient handling of common security events and tasks. **Stakeholder Engagement & Management** • Act as the primary liaison between the cyber security team and business units, IT teams, and external partners. • Develop and maintain strong working relationships with both technical and non-technical stakeholders. • Set and manage stakeholder expectations, including early problem-solving and moderating complex or high-risk discussions. • Represent cyber security in organisational forums to ensure security is considered in projects and operational decisions from the outset. • Promote a shared responsibility model for cyber security across the organisation. **Risk Communication & Ownership** • Supporting the team to ensure cyber security risks are clearly communicated, understood, and appropriately owned by the business. • Advise and influence risk owners to implement proportionate remediation actions. • Escalate critical risks where required to ensure visibility and action. **Continual Service Improvement** • Establish, track, and report against clear performance metrics for team activities, including SLAs and KPIs. • Use data and trend analysis to identify service gaps, control weaknesses, and improvement opportunities.

	• Encourage the reduction of manual effort and reactive work through automation, tooling, and process improvement. • Lead regular reviews of service and incident data to drive enhancements to the organisation's security posture. The responsibilities described are not a comprehensive list and additional tasks may be assigned from time to time that are in line with the level of the role.
Know-How [s] is used to denote the minimum shortlisting criteria.	**Essential** • Strong leadership and people management skills with a growth mindset that constantly challenges and improves how the team delivers and operates [s]. • Proven experience managing a security operations or cyber team, including coordinating multi-disciplinary security staff and resources to maintain service performance and availability [s]. • Broad knowledge of IT systems and cybersecurity principles, threats, and technologies, including network security, cloud security, endpoint protection, identity and access management, vulnerability management, sufficient to engage credibly with technical specialists and support decision-making [s]. • Extensive experience overseeing response to security incidents and ensuring operational preparedness for threats [s]. • Experience implementing service improvements and governance in a security context, such as maintaining the security knowledge base or service catalogues, ensuring technical changes follow proper governance, and driving ongoing improvements in security processes and controls. • Experience in security risk management and compliance, ensuring that security controls and operations align with organisational risk appetite and standards, such as ISO 27001 and Cyber Essentials [s]. • Able to build strong relationships and communicate security issues in clear, accessible language to senior leaders, non-technical colleagues, and external partners. • Skilled in negotiating and influencing across a diverse range of stakeholders, including handling difficult conversations to ensure that security risks and necessary mitigations are fully understood and agreed. • Good understanding of IT service management and operational planning principles, including familiarity with frameworks and tools, such as ITIL incident & change management processes, to manage and improve service reliability. • Experience implementing or maturing service management disciplines, such as ITIL processes, performance metrics, and continuous improvement programs, to achieve higher service quality and consistency [s]. • Able to analyse performance data and implement appropriate KPIs and SLAs for the team's services. **Desirable** • Background in leading teams through change, such as implementing new processes or security tools, and guiding teams through service transitions or evolving requirements. • One or more relevant professional qualifications or certifications in information security or service management, such as CISSP, CISM, CISMP or ITIL v4 Foundation or higher.

	• Experience in a humanitarian, non-profit, or public sector with understanding of the unique cybersecurity challenges and stakeholder considerations in such contexts.
Additional Requirements	None

Pre Engagement Checks Highlight bold as required		
DBS- England & Wales	None	
PVG- Scotland	None	
Access NI- Northern Ireland	None	
Driver Check	No	
<u>International Roles Only</u>		
International Police Check	No	
International Driving Licence for manual cars	No	

Role Reference		**Review Date**	

We guarantee an interview to disabled candidates (as defined in the 2010 Equality Act), who meet the minimum shortlisting criteria in the advertised person specification and apply under the disability confident scheme.