**ROLE PROFILE**

|  |  |  |  |
| --- | --- | --- | --- |
| **Role Title** | Cyber Risk Specialist | **Location** | Bristol or London |
| **Business Unit** | Technology | **Job Family** |  |
| **Reports to Role Title** | Chief Information Security Officer | **Sub Family** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **PURPOSE** | | | |
| The purpose of this role is to identify, assess, and manage cyber risks associated with third-party relationships and supply chain activities. The Cyber Risk Specialist will work closely with various departments to ensure that supply chain risks are mitigated and that the company's digital presence and customer engagement are protected.  **Purpose**   * To support the Technology team in ensuring that corporate IT systems and controls are tested, assured, represented and reported accurately and appropriately * To engage, support and work closely with the business at all levels to ensure information security regulations, requirement and policies are understood, communicated, & implemented effectively across all business functions * Support security operations and cyber incident management * Create awareness and training material, drive user compliance activities and contribute to a culture of Information security management | | | |
| **CORE ACCOUNTABILITIES** | | | |
| The Cyber Risk Specialist will:   * Conduct thorough risk assessments of third-party vendors and suppliers to identify potential cyber threats and vulnerabilities * Develop and implement risk management strategies to mitigate identified risks in the supply chain * Collaborate with Procurement, Data Protection, and Risk teams on supplier due diligence activities * Monitor and evaluate the effectiveness of technical security controls related to supply chain activities * Provide regular reporting on supply chain risk management activities and recommend improvements where necessary * Support incident investigations related to supply chain cyber threats and assist in the remediation of any findings * Create awareness and training materials to drive user compliance and contribute to a culture of information security management * Stay updated on industry best practices and standards related to supply chain risk management and incorporate them into the company's policies and procedures | | | |
| **CONTACTS/ KEY RELATIONSHIPS & NATURE OF INFLUENCE** | | | |
| **Internal:**   * IT Support & Technical Teams * Senior Management   **External:**   * 3rd Party Service Providers | | | |
| **KNOWLEDGE/ EXPERIENCE/ SKILLS** | | | |
| A good understanding of the following:   * Endpoint security * SIEM platforms * Windows Server technologies, Active Directory and Entra ID * Networking concepts (DNS, IP, segregation techniques) * Cloud computing concepts and service models IaaS/PaaS/SaaS * Authentication concepts (Windows, Entra ID, Managed Identity) * Microsoft 365 security and compliance * MITRE ATT&CK Framework * Cyber Essentials/Essentials Plus, GDPR, ISO 27001 and other information security-related regulatory and compliance standards | | | |
| **PROFESSIONAL QUALIFICATIONS & EDUCATION** | | | |
| * A degree in Cyber Security, Information Technology, Computer Science, or a related field is preferred * Relevant certifications such as CISSP, CEH, GCIH, or equivalent are highly desirable | | | |
| **TECHNICAL/ BEHAVIOURAL/ PERSONAL COMPETENCIES** | | | |
| * To have a genuine passion for Cyber Security and its technology, and a drive to continually develop professional and personal knowledge in this fast-moving area * Be self-motivated and able to work to a high standard under own initiative * Able to pay and maintain close attention to detail * Have sound analytical skills; able to think laterally and challenge existing concepts * Be a good and confident communicator at all levels; an ability to assert and defend a point of view that can be balanced with pragmatism at times * Must be able to operate as a member of the wider Technology team, contributing to a wide range of Information Security risks and issues, to provide joint outcomes * Have the ability to understand technical complexities and issues, and be able to explain and translate these to a less technical audience * Have a good understanding of security threats, attack scenarios, intrusion detection techniques and incident management * Awareness of information risk, assurance and information security strategy programs, within large corporate environments is desirable * Awareness of information security principles (Confidentiality, Integrity, Availability) * Awareness of communication channels and methods of influence (Awareness, Behavior, Culture) * Awareness of web apps design, development and deployment across different platforms * Awareness of enterprise technologies including associated security vulnerabilities and exploits | | | |
| **BUSINESS SPECIFIC REQUIREMENTS (Optional Section)** | | | |
|  | | | |
| **OPERATING ENVIRONMENT & CONTEXT:**  **TRAVEL & OTHER REQUIREMENTS** | | | |
| **ROLE DIMENSIONS** | | | |
| No of Direct Reports | 0 | Financial Impact (Direct) |  |
| Total Team Size | 5 | Financial Impact (Indirect) |  |
| No of Locations |  | Other/ People Manager (yes/ no) |  |

Back Office Use only:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Job Code** |  | **Reward Level** |  | **TW Grade** |  |
| **Salary Survey Ref** |  | **Career Level** |  | **Date Created** |  |
| **Salary Min** |  | **Salary Mid** |  | **Salary Max** |  |