THREE CROWNS LLP

ROLE PROFILE: **INFORMATION SECURITY LEAD**

LOCATION: **LONDON**

Three Crowns overview

Three Crowns is a law firm that was founded in 2014 by specialist international arbitration advocates in the belief that international disputes call for focused advice and advocacy. The firm engages primarily in complex, high-value disputes, and counts among its clients many industry leaders and sovereign states. The firm has grown significantly in each of its offices – London, Madrid, Paris, Singapore and, Washington DC – and now comprises over 140 people, including 16 partners. Across jurisdictions, it is regarded as a market leader.

The firm seeks to hire an Information Security Lead in the London office.

The role

A key member of our Information Technology team, the Information Security Lead will implement and maintain cybersecurity measures to protect sensitive legal data and client information. The role will be critical in ensuring the Firm's digital and physical assets are secured against emerging threats and comply with legal industry standards and regulations. Performing daily investigation of security incidents, security assessments and audits. The role holder will also work with relevant teams around the firm to ensure that appropriate operational security controls are understood, agreed and implemented.

Given the international nature of the firm, flexibility both in terms of hours and travel (including international) is vital.

The responsibilities of the Information Security Lead will include, but are not limited to:

- Managing intrusion detection/protection systems, firewalls, web filtering solutions, web application firewalls, host intrusion protection, antivirus, anti-malware and zero-day threat protection services., including maintaining the documentation of all services.

- Being a key resource for audits and ensure compliance is maintained to a high level.

- Maintaining the most appropriate security designs to support the firm, conduct reviews regularly considering established best practices and new technologies.

- Understanding and application of business goals and place security has in achieving them.

- Working with IT staff and other departments to enhance security and manage and track cybersecurity awareness training, working with firm leaders to improve employee resistance to phishing attacks.

- Developing, maintaining, and testing the Firm’s business continuity and disaster recovery plans to ensure minimal disruption to operations and rapid recovery in the event of a security breach or other emergencies.

- Developing and maintaining an incident response plan, conduct regular simulation exercises, and help guide the response to cybersecurity incidents to minimise impact.

- Monitoring the firm's network for unusual or suspicious activity, investigate and respond to security breaches or intrusions.

- Developing and implementing comprehensive cybersecurity policies and procedures in accordance with legal industry best practices.

- Conducting regular security audits, risk assessments and penetrations tests to identify vulnerabilities and recommend corrective actions.

- Ensuring compliance with data protection laws (e.g., GDPR) and related industry regulations.

- Responding to client security audits and take lead in maintaining the firm's compliance with third party security standards compliance (e.g., ISO 27001, Cyber Essentials, etc.)

- Providing regular reports to senior management on the Firm’s cybersecurity posture status.

- Managing relationships with security vendors, ensuring that their services and products effectively meet the Firm’s cybersecurity needs and compliance standards.

- Continuously pursuing education and staying informed about the latest innovations in cybersecurity to maintain and enhance the Firm’s security posture.

- Staying actively engaged with the latest technologies and cybersecurity trends to protect the Firm against emerging threats.

Skills and knowledge

The Information Security Lead will possess:

- At least five years' experience in an IT security position, preferably in a professional partnership.
- Familiarity with regulations and standards pertaining to data privacy and security.
- Proven experience in working with mixed project teams to define system security requirements.
- A deep understanding of European Union cybersecurity frameworks and regulations, including GDPR and ISO 27001.
- Certifications in GIAC GSEC, Sec+, SSCP, CISSP, Microsoft Certified Cybersecurity Architect Expert or similar certification preferred.
- Proven experience in security planning and development for a growing IT department.
- Experience in designing security solutions with hands on experience of implementation.
- A strong analytical approach to problem solving.
- The ability to work in a fast paced and dynamic environment.
- The skills to quickly identify root causes and provide possible solutions.
- Excellent documentation skills and capable of creating security architecture diagrams.