Regional CISO - China

Location: **Shanghai**
Starting date: **ASAP**

ABOUT THE COMPANY
Our client is a global aerospace equipment manufacturer.

Role Overview
As Regional CISO for China, you will lead the implementation of the company's global information security strategy across China. You will be the key link between regional business leadership and Corporate Information Security (CIS), ensuring security priorities support business needs and that regional risks and requirements shape the global security agenda.
This is a business-facing leadership role combining strategy, risk management, stakeholder engagement and regional execution. You will work across a diverse, decentralized organization, bringing together business, IT and security teams to strengthen cyber resilience and enable secure business growth.

RESPONSIBILITIES

- Regional strategy and roadmap: Translate global CIS strategy, policies and standards into a practical China roadmap aligned with business priorities, the threat landscape and local regulatory requirements.
- Regional security team and transformation: Establish and build the China Regional Security Team as an integral part of global CIS functions. Lead successful transition and transformation activities, building direct links with the business and aligning regional capabilities with global CIS functions.
- Business and executive partnership: Build and maintain direct links with business leaders to understand and address business requirements and needs. Advise management of the region and entity leadership on material cyber risks, priorities, investment needs, decisions and dependencies.
- Lead regional security governance: Establish and chair the regional information security committee, report on security progress and risks, and escalate material matters to the Global CISO and relevant global governance forums.
- China cyber and data regulation: Coordinate security implementation with Legal, Data Protection and accountable business owners across the PRC Cybersecurity Law, Data Security Law, Personal Information Protection Law, MLPS 2.0, applicable CAC requirements, important-data considerations, cybersecurity incident obligations and cross-border data-transfer controls.
- Risk, assurance and remediation: Coordinate regional risk assessments, audits, certifications, customer requirements and remediation, ensuring clear ownership and visibility of significant regional risks. Maintain ISO/IEC 27001 certification for

certified operations within the regional scope, coordinating surveillance and recertification audits, corrective actions and continual improvement.

- Secure transformation and capability adoption: Embed Security by Design into cloud, digital, OT, manufacturing, connected-product and third-party initiatives, and drive adoption of global CIS services, standards, awareness and resilience measures. Work with global CIS functions, Legal, Data Protection and business owners to adapt global solutions to local business and regulatory needs.
- Incident and crisis coordination: Act as the regional leadership coordination point during material cyber incidents, linking affected entities with global CIS response capabilities and supporting decisions, communication, regulatory alignment and recovery priorities.
- Leadership and operating model: Provide functional direction to designated China security personnel, directly manage assigned regional employees and maintain clear boundaries among CIS, IT, divisions, legal entities and business risk owners.

REQUIREMENTS

- Bachelor's or master's degree in cybersecurity, information technology or a related field, or equivalent relevant professional experience.
- At least 10 years of relevant experience in information security, cyber risk or security governance, including five years in leadership.
- Experience working in a global company with established, integrated operations in China is highly valued, preferably in a manufacturing context. Practical knowledge of the CSL, DSL, PIPL, MLPS 2.0, CAC requirements and cross-border data controls is required.
- Strong ability to engage senior executives and translate cyber, regulatory and technical matters into clear business decisions, priorities and accountable actions.
- Broad knowledge of security governance, risk management, incident and crisis coordination, Security by Design, ISO/IEC 27001 and NIST CSF.
- Experience with manufacturing, industrial operations, OT, product security, supply-chain security or similarly complex environments.
- Professional fluency in English is required; Mandarin Chinese proficiency is strongly preferred.
- CISSP, CISM, CISA, CRISC or an equivalent internationally recognized certification is strongly preferred.
- Willingness to travel within China and internationally as required.
- Languages: Chinese and English are a must, German is an advantage.

APPLICATION

Please send your CV in English to: sh-recruitment@ccifc.org.