HOXHUNT

Head of Human Risk

/ Human Risk Manager / Human Risk Officer

Role

The Head of Human Risk is a senior leader who oversees and coordinates the cybersecurity human risk management strategy and activities across the organization. The Head of Human Risk is responsible for identifying, assessing, mitigating, and reporting on the human factors that affect the cybersecurity posture and resilience of the organization.

Responsibilities

The Head of Human Risk:

- **Develops and implements a human risk management strategy** that aligns with the organization's business objectives, risk appetite, and cybersecurity policies and standards; and reviews the strategy at least once per year.
- **Establishes and maintains a continuous register quantifying the main human risks for the organization,** including factors such as people's attitudes, knowledge and behaviors related to security.
- **Designs and delivers human risk management initiatives that foster a positive security culture** and the adoption of secure habits among employees, contractors, partners, and customers:
  - 👉 Ensures the organization complies with the security awareness requirements of applicable regulations, frameworks and standards.
  - 👉 Deploys targeted training where the risk lies, to the right people at the right time. This could take the form of nudges, in-person trainings, e-learnings, videos, games, events, etc.
  - 👉 Fosters a positive culture of security where all employees feel responsible and empowered to tackle the cybersecurity risk, and are rewarded for doing so. Develops and maintain a security ambassador network to support the human risk management team in their initiatives.
  - 👉 Reduces frictions in security with activities such as policy reviews and simplification, new tools deployment, communication and outreach support for the security team, collaboration with external teams to improve UI/UX experience etc.
- **Coordinates and collaborates with other key stakeholders,** such as the CISO, IT, HR, Legal, Compliance, and Business Units, to ensure a holistic and consistent approach to human risk management.
- **Monitors and reports on human risk performance and metrics,** and provides recommendations and guidance for continuous improvement and risk reduction. Shares metrics with relevant stakeholders to empower them in activities in their departments or regions.
- **Leads a multidisciplinary team of experts** that can include cyber-psychologists, communication experts, learning instructors, security specialists, project managers, data analysts etc.; and supports the continuous development of this team.
- **Manages the human risk management program's budget** and continuously improves the efficiency of the program.
- **Ensures leadership support for human risk management-related initiatives,** and enables organization leaders with the knowledge and tools to set the example for the organization.
- **Stays abreast of the latest trends, best practices, and emerging issues** in human risk management and cybersecurity.

Reporting

The Head of Human Risk reports directly to the Chief Information Security Officer (CISO) / Head of IT Security. This allows for increased collaboration with the rest of the Cybersecurity team, and better reporting to the C-suite or board. He/She is expected to establish a Human Risk Management Steering group and independently facilitate and report to the senior leader chairing the SG.

Qualifications

- **Bachelor's degree or higher in a relevant field,** such as psychology/behavioral science, engineering, communications or cybersecurity.
- **Minimum of 3 years of experience** in human risk management, or 5+ years in related fields.
- **Excellent communication, presentation, and interpersonal skills,** with the ability to influence and engage diverse audiences and stakeholders.
- **Data-driven approach** and strong analytical, problem-solving, and decision-making skills, with the ability to balance risk and business needs.
- **Proven experience in leading and managing a team,** as well as overseeing the budget and resources.
- **High level of integrity, ethics, and professionalism**, with the ability to handle sensitive and confidential information.
- **Optional:** professional certification in human risk management, cybersecurity, or related fields, such as SANS Security Awareness Professional (SSAP), Infosec Certified Security Awareness Practitioner (CSAP), NICCS Certified Cybersecurity Awareness Professional (CCAP), CISSP, CISM.