Job Title: Business Information Analyst - Cyber Security
Location: Bangalore

ABOUT UNILEVER:
Be part of the world’s most successful, purpose-led business. Work with brands that are well-loved around the world, that improve the lives of our consumers and the communities around us. We promote innovation, big and small, to make our business win and grow; and we believe in business as a force for good. Unleash your curiosity, challenge ideas and disrupt processes; use your energy to make this happen. Our brilliant business leaders and colleagues provide mentorship and inspiration, so you can be at your best. Every day, nine out of ten Indian households use our products to feel good, look good and get more out of life – giving us a unique opportunity to build a brighter future.
Every individual here can bring their purpose to life through their work. Join us and you’ll be surrounded by inspiring leaders and supportive peers. Among them, you’ll channel your purpose, bring fresh ideas to the table, and simply be you. As you work to make a real impact on the business and the world, we’ll work to help you become a better you.

At HUL, we believe that every individual irrespective of their race, colour, religion, gender, sexual orientation, gender identity or expression, age, nationality, caste, disability or marital status can bring their purpose to life. So apply to us, to unleash your curiosity, challenge ideas and disrupt processes; use your energy to make the world a better place. As you work to make a real impact on the business and the world, we’ll work to help you become a better you!

Unilever’s Cyber Security organization is a multi-disciplinary team responsible for protecting the Confidentiality, Integrity and Availability of our Information and Operations. Our Cyber Security organization runs a 24x7 Security Operations Centre (SOC), oversees a robust Security Architecture and associated technology landscape, provides Cyber Security Solution Engineering and Risk Advisory to our business, and assesses the security of our vast technology estate, including factories, to name but a few areas. Cyber Security sits as part of the Business Operations organisations, as a peer to Unilever’s Technology and Data functions and the broad Supply Chain agenda. Cyber Security is tasked with elevating, reporting on and influencing enterprise cyber security risk mitigation across Unilever. The Cyber Security function is made up of the Governance, Risk, Assurance, and Compliance (GRAC) team, the Tech & Ops team, the BISO teams, and the Office of the CISO.

Role Purpose:

This Business Information Analyst role will support Unilever’s BISO for North Asia, South Asia, and South East Asia. The role will include supporting in cyber analysis and reporting across the region, and support in some risk management activities as well. These activities will be conducted with a ‘Risk Based’ approach to help individual businesses manage cyber risk in their area.

Role Summary:

A vacancy exists for Business Information Analyst for North Asia, South Asia, and South East Asia within Unilever’s cyber function. The successful candidate will support Unilever’s cyber function in the region in achieving and maintaining Cyber Security objectives, standards, awareness, and compliance, defined using a ‘Risk Based’ approach through timely and actionable report creation and socialisation. This role will partner with the BISO for Acquired Businesses to support in delivering services to the Acquired Businesses in the region. This analyst position will report to the regional Business Information Security Officer.

Key areas delivered by the BISO team that will be supported by this role’s reporting will include:

Cyber security solution engineering and risk advisory across Unilever business in region of responsibility, assuring appropriate risk identification, assessment, mitigation, and reporting.
Ensuring the deployment and running of security tooling in the regions, in conjunction with the Security Tech & Ops team.
Ensuring the Security Operations Centers (SOC) have full visibility across the ecosystem and actively participate in incident response at the direction of the Head of Incident Response.
Developing and delivering risk reports to the region.
Tailoring cyber training and awareness across the region in alignment and partnership with the Cyber Training and Awareness Lead.
Leading cyber cultural transformation across the region in line with our Security Strategy and Transformation program.
Maintaining and effectively directing the timely closure of security exceptions in businesses while reporting status to the Governance, Risk, Assurance and Compliance (GRAC) team.
Providing standards and controls feedback, based on local implementation requirements to the GRAC team to help shape global policies and standards.
Partnering with the BISO for Acquired Businesses to ensure appropriate cyber risk mitigation is ongoing for acquired businesses in their regions of responsibility.
Partner with the BISO for Supply Chain and ISO for R&D to ensure appropriate cyber risk mitigation for those functional areas within his/her region of responsibility.
Testing resiliency (including business continuity planning (BCP) and disaster recovery (DR)) in the region of responsibility.

Main Accountabilities
Responsible for supporting the BISO in data gathering, report creation, and presentation for the region.
Responsible for supporting the BISO in cyber risk reporting across the region to the CISO and to the regional business leaders.

Key Skills and Relevant Experience
Skills:
Excellent written and verbal communication skills and able to be understood by both technical and non-technical personnel.
Proven ability to lead, develop, and motivate a team.
Ability to manage conflicting priorities and multiple tasks.
Skilled with Excel, Power BI, and PowerPoint.
Strong data management and analysis skills
Stakeholder management and interpersonal skills at both a technical and non-technical level.
Ability to work in a collaborative environment with international team members.
Outstanding critical reasoning and problem-solving skills – sticking to the problem until it is resolved.
Customer-orientated, whether responding to queries or delivering new services.
While Unilever’s primary language is English, business language proficiency in additional regional languages is preferred.

Experience:
The role holder will have ideally have previously held a role in Cyber Security or have a passion to learn more in the area.
Experience driving a complex change agenda, and an ability to challenge the “status quo”.
Strong strategic and operational business awareness, with an understanding of the key drivers, levers, issues, and constraints of digital businesses.
Experience within a customer focused environment.

Behaviours
Candidates would be required to demonstrate the Unilever Standards of Leadership & live the Values through showing the following behaviors:
Agility – Flexes leadership style and plans to meet changing situations with urgency. Learns from the past, envisions the future, has a healthy

dissatisfaction with the status quo.
Personal Mastery – Actively builds wellbeing and resilience in themselves and their team. Has emotional intelligence to take feedback, manage mood and motivations, and build empathy for others. Sets high standards for themselves and always brings their best self.
Passion for High Performance – Inspires the energy needed to win, generating intensity and focus to motivate people to deliver results at speed.