Cyber Resilience Officer Job Description

Introduction

This is a sample job description which outlines the role of a Cyber Resilience Officer (visit www.cyberresilienceofficer.org for more details), a pivotal and emerging position that we advocate for global adoption. Embracing this role is a strategic move to fortify an organization's resilience posture against the ever-evolving digital threats.

Overview

The Cyber Resilience Officer is accountable for the organization's ability to manage cyber resilience and for implementing cyber resilience goals. The role should have regular Board access, sufficient authority, command of the subject matter, experience, and resources to fulfil these duties.

The organization has mechanisms in place for providing the Cyber Resilience Officer ready access to each of the following: communication with the Board of Directors; empowerment over cyber resilience strategy, management, and enforcement actions; cyber resilience expertise and executive training; the acquisition of personnel, financial and technology resources.

The role seeks to:

- Continuously understand and uplift the organization's cyber resilience posture.
- Answer the question – Could we be the next victim of extreme but plausible cyber threats?
- Shape the reporting of cyber resilience risk at risk forums across the organization to drive awareness and change.

Responsibilities

This requires an individual who can work across the various lines of defence and bring expertise and analysis in the area of cyber resilience:

- Understand current cyber threats and the technical aspects of the attacks used.
- Provide oversight and influence of the organization's cyber assessment capabilities.
- Participate within threat action groups targeting cyber resilience related threats.
- Work with reporting and analytics teams to produce innovative risk reports related to cyber resilience.
- Mix quantitative and qualitative metrics to measure cyber resilience exposure in a non-technical way.
- Identify and collate cyber resilience requirements in support of enterprise security architecture engagements.
- Lead through influence and collaboration supporting constructive input and challenge.
- Collaborate and influence colleagues across various lines of defence including CISO and CIO teams.
- Continuously identify critical 3rd parties, deeply understand of the organization's important business services.
- Set impact and risk tolerances, monitor threshold levels and contingency plans for important business services (including third parties).

Qualifications

- Proficiency in the main cyber resilience frameworks like NIST 800-160, MITRE CREF and NIST 800-172.
- Have significant experience working in cybersecurity threat management.
- Experience of the tactics, techniques and procedures used by advanced cyber adversaries.
- Experience of cyber resilience strategies, design, engineering and architecture.
- Significant technical expertise and able to communicate in depth with colleagues from blue teams, purple teams and red teams.
- Ability to focus on extreme but plausible threats as well as other possible threats.
- Experience in third party risk management and mapping of services to assets (people, assets, technology, vendors etc).
- Able to communicate to technical and non-technical audiences, able to explain complex topics with simplicity.
- Able to articulate requirements clearly to non-cyber experts spanning data analytics, reporting and risk to ensure resultant cyber resilience reports are consumable and relevant.