IIET Executive Workforce Cybersecurity Defence Programme

Theme: Developing a sound strategic cybersecurity defence programme for the workforce in public, private and academic sectors

Executive Summary

Cyberattacks are today persistent, undermining digital society's gains. Equipped with superior tools and abilities, cybercriminals are becoming more sophisticated, employing advanced tools like artificial intelligence (AI) and machine learning (ML) to automate and escalate attacks. State actors and well-funded cybercrime syndicates also conduct highly-targeted and persistent cyberattacks.

Several inter-related factors contribute to the unrelenting nature of cyber events. Research has proven that despite technological advancements and security protocols, people remain the most vulnerable point in cybersecurity because human emotional intelligence and behaviour are unpredictable and challenging to control entirely.

Therefore, creating a robust cybersecurity workforce is the most significant first line of defence. However, governments and organizations face the challenge of building skilled workforce capacity that can match the pace and dimensions of cyber threats. This challenge is due to several factors, such as Cybersecurity being a new field with complexities, across knowledge domains. Increasingly, most nations and organisations misdirect their energy on building capacity along generic (or unstructured and uncategorised) one-cap-fits-all mindset.

A more strategic and effective approach is the understanding that building a robust National Cybersecurity Workforce (NCW), requires adequate grasp of the tasks, knowledge and skills (TKS) needed to create a competent and resilient cybersecurity defence workforce.

This is the thrust of the IIET in curating this comprehensive executive masterclass; The IIET Executive Workforce Cybersecurity Defence programme. It is conceptualized as a beacon to face head-on, the prevailing cybersecurity workforce challenge. Further more, it seems to enable Governments and organisations in the public, private, and academic sectors develop a robust cybersecurity defence workforce pipeline that is skilled and competence-based. Currently, the emphasis on cybersecurity capacity building has predominantly centred on the middle and lower echelons of the workforce alone, leaving out decision makers. Those responsible for directing cybersecurity initiatives should understand the various TKS that can thwart present and future cyberthreats. This masterclass aims to strategically fill this gap. The programme will equip top-decision makers, managerial and directorate cadre personnel to establish and align with a common lexicon that describes cybersecurity work and workers, regardless of where the organisations' work is performed.

> "It is certain that significant challenge facing cybersecurity posture today is a dearth of the required pool of knowledgeable, competent, and skilled workforce adequate to navigate the present and emerging dynamics of the cybersecurity defence ecosystem. Current approaches misdirect energies on building capacity along a generic (or unstructured and uncategorised) one-cap-fits-all mindset."

Prof. Lucia Abrahams
Director, LINK Centre, University of Witwaterstrand, Johannesburg South AFrica

Suite 011, Nimota Plaza, Plot 855, Tafawa Balewa way, Area 11, Garki, Abuja

07052500468, 08163378811 https://iiet.ng

Target Audience

The programme targets the decision-making cadre—managers and directors formulating cybersecurity policies and strategies; drawn from the Cybersecurity, ICT, and HRM departments. The Programme recognizes that cybersecurity defence requires coordination across departments.

Training Methods

- A blend of masterclass methods, designed to interrogate and deliver effective practical solutions as well as create value.
- Instructor-led sessions: Expert-led masterclass on core tenets of cybersecurity workforce taxonomy.
- Use case simulations: Use case interactive exercises to reinforce technical skills.
- Group discussion: Opportunities for collaboration, critical thinking, and peer learning.
- Assessment and certification: Pre- and post-masterclass assessments to measure knowledge gained, with certification provided upon successful completion.

Objective

The primary objective of this programme is to enable cybersecurity policy makers, managers and directors develop a vasertile and well-horned workforce that understands contemporary cybersecurity defence tasks, knowledge and skills required to be on top of cybersecurity defence programme. Specific objectives include:

- Build core cybersecurity functions spanning the cybersecurity defence ecosystem and equipping participants with the technical, analytical, and strategic knowledge to define and create a competent workforce.
- Build a cybersecurity risk-aware defence workforce that continuously understands the dynamic threat and risk landscapes, vulnerability management, and risk mitigation strategies.
- Develop repeatable and responsive cybersecurity defence workforce needs assessment metrics and framework.
- Develop rganisation-wide cybersecurity defence ocapacity that aligns with tasks, knowledge, and skills (TKS).
- Understand international cybersecurity frameworks, legal compliance, and governance standards.

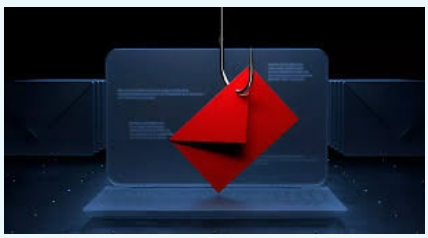
Expected Outcomes

Upon completion of the masterclass, participants will be able to:

- Identify core cybersecurity TKS that align with their organisation's vision and mission.
- Implement Cybersecurity defence workforce, based on functions and roles.
- Develop repeatable cybersecurity defence workforce needs assessment metrics and framework.
- Implement a cybersecurity defence risk-aware workforce that continuously understands the evolving vulnerability, threat and risk landscapes.
- Demonstrate cybersecurity defence governance proficiency in using key personnel and resources as part of cybersecurity risk management.

Masterclass Modules

This executive masterclass is divided into seven modules that align with standard cybersecurity defence workforce functions.



Masterclass Fee

Per participant: N500,000.00
2 to 4 Participants: N450,000.00
Above 5 participants: N400,000.00

Masterclass Package

Masterclass bag
Masterclass materials (soft copy)
Lunch / Tea breaks

NOVEMBER 25 – 29TH, 2024

VENUE: Redisson, Hotel, Ikeja Lagos