Cybersecurity

PROSPECT ACADEMY

PRINCIPLES OF CYBERSECURITY FOR MIDDLE MANAGEMENT

Elevate Your Cybersecurity Leadership

WHAT'S IN IT FOR ME?

In today's digital landscape, the demand for executive-level cybersecurity proficiency is not just necessary—it's imperative. This workshop is designed specifically for lower to mid-level managers aiming to refine their cybersecurity capabilities and leadership in the increasingly complex cyber environment.

What You Will Gain

- Applying the Security Principles, Risk & Governance
- Applying Data Security & Privacy
- Applying Access Controls Concepts (Physical & Logical)
- Applying Network Security
- Applying Cloud Security
- Applying Security Operations

COURSE OVERVIEW

This **Three-days'** workshop covers the six key elements of cyber security. The course emphasizes on the building the application skills of cybersecurity principles, concepts, theories, and models. The key focus is on establishing the practices on: GRC, data privacy, and security operation. Establishing the access and security controls. Enables the organization to inculcate practices regarding network and cloud security. It prepares candidates to become a part of a dynamic and rewarding workforce in Cybersecurity. Enables them to demonstrate the relevant technical knowledge, abilities, and skills.

COURSE OUTCOMES

Participants will emerge with the ability to:

- Possess the skills in various roles required in Information Security
- Gain competitive advantage in career progression to stay employable
- Implement and Operate the Cyber-Essential and Cyber-Trustmark standards
- Apply the knowledge to prepare for Professional Certification, CISSP
- Qualify to appear in the ISO 27001 Lead Implementer training
- Qualify to appear in the ISO 27001 Lead Auditor training
- Gather experience to progress to the next level of Security Management

COURSE DURATION

Three (3) Days / Twenty-Four (24) Hours

COURSE FEE

SDG1,050.00 before GST

COURSE OUTLINE

Topic 1 - **Security Principles**

Understand the security concepts of information assurance.
- Basic concepts and theory

Understand the risk management process
- Risk management

Understand security controls
- Different types and styles of Controls

Understand governance
- Policies, Procedures, Standards, Regulations and laws

Exposure to security architecture and frameworks
- Architecture and Frameworks

Topic 2 - **Understanding Data Security & Privacy**

Understand data security
- Encryption, Data handling, and Security events

Understand Data Privacy
- Purpose, Importance, and Components
- GDPR highlights

Topic 3 - **Access Controls Concepts**

Understand physical access controls
- Physical security controls and monitoring

Understand logical access controls
- Principle of least privilege and Segregation of duties
- Primary access control types

Topic 4: **Network Security**

Understand computer networking
- Purpose and Applications

Understand network threats and attacks
- Types of threats (DDoS, virus, worm and more)
- Identification and Prevention

Understand network security infrastructure
- Network segmentation (segregation, isolation)
- VLAN, VPN, and NAC

Understand network Attacks and Mitigations
- Phishing (Social Engineering)
- Distributed Denial-of-Service (DDoS)
- Malware and more...

Topic 5: **Cloud Security**

Understand the concept and models
- Definition and features
- Service Models and Delivery Models

Understand Virtualization
- Hypervisor (type 1, type 2)
- Virtualization

Understand Securing the Cloud
- Infrastructure, Data, and Application
- Security as a Service (SecaaS)

Understand Threat, Risk, Compliance
- Cloud Threats and Risk Management
- Cloud Compliance (Audit and Governance)

Understand Operation and Service Management
- Cloud Service Provider (CSP)
- Cloud Incident Management and Shared Responsibility Model

Topic 6: **Security Operations**

Understand Incident Response
- Incident Response Steps
- Change & Configuration management
- Investigation and Forensics

Understand BC & DR
- Purpose, Importance, and Components

Understand 3rd Party Security
- Contract, SLA, and MOU/ MOA

Understand security awareness training
- Purpose, Importance, and Components

COURSE OBJECTIVES

It is intended for lower to mid-level managers who are designated to design, build, and operate cybersecurity capability of an organization. These IT or IT/Cyber security managers are tasked to lead and manage technical teams who are either internal or outsourced from System Integrators. They are responsible for constructing the Information / Cyber objectives, goals, and strategy on behalf of the functional management under a CISO/CIO. They are required to participate and manage the Governance, Risk, and Compliance (GRC) functionalities. They participate to formulate the relevant policies, procedures, guidelines, and operational documents. They recommend the relevant frameworks, models, and methods. They are responsible for creating cyber security awareness and knowledge for all the employees. To ensure a culture of good Cyber Hygiene and ethics. This will cause the organization's cybersecurity posture to improve. They thrive to inculcating the practice of "See something, do something" among all employees.

WHO SHOULD ATTEND?

- IT Professionals/Managers: Those looking to enhance their cybersecurity skills and take on leadership roles
- Career Transitions: Ideal for professionals transitioning into the cybersecurity field

PRE-REQUISITES

- You identify yourself as a problem solver, analytical and a critical thinker, and a team player
- You possess a any post-graduate diploma and/or a certification in Information Technology

READ NOW

REGISTER NOW

2, Alexandra Rd, #03-01B Delta House,
159919, Singapore
+65 9239 5917
prospectprotection.net