email : techcenter@trainocate.com.my
contact : +603-2281-1111

CWB: CyberSecurity Workshop for Business

Course Code: CWB
Duration: 1 day
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

This Workshop aims to stimulate the intensity and need of Cyber Security among the business user. This workshop is designed to give an exposure on IT Systems Security & Infrastructure, Monitoring Potential Threats and Attacks.

Each and every organisation is accountable for ensuring that their systems are secure. A company's success is directly proportional to its ability to prevent the corruption or even theft of its information systems. Not only will increasing efficiency and productivity result from the implementation of effective security measures, but it will also provide protection from liability.

You need to have a solid understanding of the fundamental ideas behind cyberspace before you can design and put into practise any preventative measures against cyberattacks. The approach (or approaches) to cyber security that an organisation chooses to implement should be adapted to meet the specific requirements of the organisation.

As was mentioned earlier, the implementation of methods to prevent attacks on a company's information systems is the essence of what constitutes cyber security. Controlling physical access to the system's hardware is one aspect of cyber security. Another aspect of cyber security is protecting against potential threats that could arise from network access or the injection of code.

Participants in our workshop will gain an understanding of both the fundamentals of protecting their computer systems as well as the methods that should be put into practise in order to achieve this goal.

SKILLS COVERED

- Identify and explain the various concepts and definitions related to cybersecurity.
- Identify and explain the security protections offered by the cloud.
- Gain an understanding of the various forms of malicious software and security breaches.
- Be aware of the different kinds of cyberattacks that could occur.
- Methods of effective prevention need to be developed.

WHO SHOULD ATTEND?

This training is intended for professionals who have full-time IT experience, and are pursuing cybersecurity knowledge to enhance credibility and career mobility. The course is ideal for those working in positions such as, but not limited to:

- IT Executive
- IT/Security Manager
- IT/Security Consultant
- IT Auditor / None IT Auditor
- IT Risk Manager/Analyst
- IT Compliance Manager /Analyst
- HOD, Senior Manager, Director and Business Owner
- Business User
- Project/Program Manager

PRE-REQUISITES

There are no prerequisite requirements for taking the course, however, in order to make full use of the course candidate should have

necessary working experience in information technology.

MODULES

Module 1: Cybersecurity Overview

- Topic 1-Introduction to Cybersecurity
- Topic 2-Cybersecurity Objectives
- Topic 3-Cybersecurity Roles

Module 2: Cybersecurity Concepts

- Topic 1-Common Attack Types & Vectors
- Topic 2-Policies & Procedures
- Topic 3-Cybersecurity Controls

Module 3: Security Architecture

- Topic 1-Overview of Security Architecture
- Topic 2-Defense in Depth
- Topic 3-Perimeter Network Defence
- Topic 4-Cloud Security
- Topic 5-Monitoring, Detection and Logging

Module 4: Security Assessment & Testing

- Topic 1-Process Controls-Risk Assessments
- Topic 2-Process Controls-Vulnerability Management
- Topic 3-Process Controls-Penetration Testing

END OF PAGE