London TDM

Information Technology and Digital Transformation Training Courses

Course Venue: United Kingdom - London

Course Date: From 10 May 2026 To 14 May 2026

Course Place: London Paddington

Course Fees: 7,500 USD

Introduction

With the increasing prevalence of cyber threats, it is crucial for IT professionals to be equipped with the essential skills and knowledge to protect their organizations. This 5-day intensive course, "Cybersecurity Essentials for IT Professionals," offers a comprehensive exploration of foundational cybersecurity concepts, facilitating a better understanding of potential vulnerabilities and the development of effective defense strategies.

Objectives

- Understand key cybersecurity concepts and terminology.
- Identify common types of cyber threats and their potential impact.
- Explore best practices for implementing cybersecurity measures.
- Gain insights into regulatory and compliance requirements.
- Learn the fundamentals of incident response and recovery planning.

Course Outlines

Day 1: Introduction to Cybersecurity

- Overview of Cybersecurity Landscape
- Key Terminology and Concepts
- Understanding Cyber Threats
- The Importance of Cyber Hygiene
- Building a Security-First Culture

Day 2: Identifying and Addressing Threats

- Common Threat Types: Malware, Phishing, Ransomware
- Vulnerability Assessment and Management
- Conducting Threat Intelligence
- Behavioral Analysis and Threat Detection
- Case Studies on Recent Cyber Attacks

Day 3: Implementing Security Measures

- Designing a Secure Network Architecture
- Encryption and Data Protection Strategies
- Endpoint and Firewall Security
- Access Control and Authentication Techniques
- Implementing Multi-factor Authentication

Day 4: Regulatory Compliance and Best Practices

- Understanding GDPR, HIPAA, and Other Key Regulations
- Developing a Security Policy Framework
- Auditing and Monitoring for Compliance
- Best Practices for Security Awareness Training
- Third-party Risk Management

Day 5: Incident Response and Continuity Planning

- Building an Incident Response Plan
- Conducting a Post-Incident Analysis
- Business Continuity and Disaster Recovery
- Tools for Incident Detection and Response
- Proactive Strategies for Future Threats