London TDM

Security Management and Risk Protection Training Courses

Course Venue: Malaysia - Kuala Lumpur

Course Date: From 02 August 2026 To 06 August 2026

Course Place: Royale Chullan Hotel

Course Fees: 6,000 USD

Introduction

This 5-day course titled "Cybersecurity Awareness for Non-IT Managers" is designed to equip managers from non-technical backgrounds with the essential understanding and skills they need to recognize and mitigate cybersecurity threats. As businesses increasingly rely on digital operations, understanding cybersecurity is crucial for protecting in-house data and maintaining the trust of stakeholders.

- Understand the fundamentals of cybersecurity and its importance in today's business environment.
- Recognize common cyber threats and vulnerabilities affecting organizations.
- Develop strategies for effective cybersecurity management and risk mitigation.
- Learn about regulatory requirements and compliance related to cybersecurity.
- Cultivate a proactive cybersecurity culture within your organization.

Course Outlines

Day 1: Understanding Cybersecurity Basics

- Introduction to cybersecurity: Definitions and concepts
- Importance of cybersecurity for businesses
- Overview of common cyber threats (e.g., malware, phishing)
- Insights into cybersecurity and data breach statistics
- Basic cybersecurity terminology

Day 2: Identifying Threats and Vulnerabilities

- Understanding threat actors and motivations
- Types of vulnerabilities within an organization
- Case studies on recent cybersecurity incidents
- Exploring the impact of social engineering attacks
- Tools and techniques used for threat identification

Day 3: Cybersecurity Management and Mitigation Strategies

- Developing a cybersecurity strategy for non-IT sectors
- Risk management and assessment techniques
- Implementing effective access control measures
- Importance of network security and monitoring
- Training employees on cybersecurity best practices

Day 4: Legal and Compliance Issues

- Introduction to cybersecurity laws and regulations
- Understanding data protection and privacy laws
- Compliance management strategies
- Implications of non-compliance
- Develop policies to support legal and regulatory compliance

Day 5: Building a Cybersecurity Culture

- The role of leadership in cybersecurity
- Encouraging a proactive cybersecurity mindset
- Strategies for ongoing cybersecurity training and awareness
- Best practices for incident response and recovery
- Measuring the effectiveness of cybersecurity initiatives