معهد المورد للتدريب
AL MAWRED TRAINING INSTITUTE

LDR512 Security Leadership Essentials for Managers

Day 1: Introduction to Cybersecurity and Risk Management

Objective: Build foundational cybersecurity awareness and understand the business impact of threats.

Session 1: Cybersecurity for Business Leaders

The evolving threat landscape

Understanding cyber terminology and principles

Managerial roles in supporting security initiatives

Session 2: Business Impact and Risk Analysis

Identifying critical assets and data

Threat and vulnerability assessment

Introduction to risk management frameworks (NIST, ISO 27005)

Session 3: Cyber Risk Appetite and Tolerance

Aligning risk with business goals

Understanding the cost of risk vs. control

Case Study: Cyber risk gone unmanaged

Day 2: Governance, Policy, and Compliance Essentials

Objective: Understand how leadership shapes governance and ensures policy effectiveness.

Session 1: Cybersecurity Governance Principles

Roles of executive leadership, board, and CISO

Information security governance models

Security governance vs. management

Session 2: Security Policy and Program Development

Elements of effective security policies

Policy life cycle and enforcement strategies

Creating a culture of security awareness

Session 3: Compliance and Regulatory Requirements

Overview of key regulations: GDPR, HIPAA, SOX, etc.

How to lead compliance efforts

Internal audit and accountability

Day 3: Cybersecurity Frameworks and Controls

Objective: Equip leaders to manage frameworks and integrate controls effectively.

Session 1: Introduction to Cybersecurity Frameworks

NIST Cybersecurity Framework (CSF)

ISO/IEC 27001, CIS Controls

Comparing and integrating frameworks

Session 2: Selecting and Prioritizing Security Controls

Control categories: preventive, detective, corrective

Defense-in-depth strategy

Risk-based control implementation

Session 3: Third-Party and Supply Chain Risk

Vendor security management

Due diligence and contract clauses

Case example: Supply chain attack fallout

Day 4: Communication, Awareness, and Incident Management

Objective: Build leadership communication skills and manage incidents effectively.

Session 1: Cybersecurity Communication for Leaders

Communicating with the board and stakeholders

Translating tech into business language

Security reporting and dashboards

Session 2: Security Awareness and Training Programs

Developing organization-wide awareness initiatives

Social engineering and phishing defense

Role-based training (HR, legal, finance, etc.)

Session 3: Incident Response & Business Continuity

Building and leading incident response plans (IRP)

Crisis communication during incidents

Business continuity and disaster recovery basics

Day 5: Cybersecurity Strategy, Leadership, and Final Exercise

Objective: Apply learned concepts in a strategic and practical simulation.

Session 1: Developing a Cybersecurity Strategy

Aligning strategy with business vision

Building a multi-year roadmap

Budgeting and resource planning

Session 2: Leading Security Teams and Culture

Security leadership principles

Collaboration across departments

Building and sustaining a security-focused culture