CONCEPT

Security Champions Programme: Building and Running a Cyber Champions Network

20 – 24 September 2027
Dubai - Five-star CBD venue



Security Champions Programme: Building and Running a Cyber Champions Network

Ref: 933_21506 **Date:** 20 – 24 September 2027 **Location:** Dubai - Five-star CBD venue **Fees:** 21450 SAR

Introduction:

A security champions programme gives a small security team eyes and ears in every department, yet many networks stall because the role is vague, champions are picked by availability and nobody can show what they changed. This Core Concept course equips awareness leads and the champions themselves to design the champion role, recruit and onboard the right people, coach colleagues on secure habits, handle first response to suspected incidents and prove impact on security culture. Participants produce a Champions Network Design and Local Awareness Plan for a case business unit.

Course Objectives:

- Define the purpose, model and charter of a security champions network that fits the organisation's structure
- Select, nominate and onboard champions with a clear role profile, stated expectations and manager endorsement
- Coach colleagues on phishing cues, account protection, data handling and device security using peer-level explanations
- Apply first-response triage to suspected incidents and route them through agreed escalation paths
- Run local awareness activities and influence colleagues, including light secure development prompts for product teams
- Measure champion impact and security culture, and sustain the network through recognition and community practice

Target Audience:

- Awareness and training coordinators who set up and run a champions network across business units
- Departmental staff nominated as the security point of contact for their team
- IT support and service desk staff who act as the first link between colleagues and the security team
- Developers, testers and product owners who promote secure practice inside delivery teams
- Operations and administrative staff who coordinate information handling for their unit

Course Outline:

Day 1: Purpose and Foundations of a Security Champions Network

- Security Champions Network Purpose: Bridging the Security Team and Business Units
- Champion Programme Models: Departmental, Product Team and Site-Based Networks
- Human Risk Drivers Behind Credential Misuse, Mis-Sent Data and Unreported Incidents
- Security Awareness and Culture Maturity Model Stage Self-Placement
- Business Unit Readiness Scan: Sponsors, Pain Points and Existing Informal Contacts

Day 2: Champion Role Design, Recruitment and Behaviour Models

- Champion Charter: Mandate, Expectations and Boundaries of the Role
- Champion Role Profile and Selection Criteria for IT-Literate Business Staff
- Manager Endorsement and Nomination Process for Champion Candidates
- Onboarding Pathway: Induction Kit, Buddy Pairing and Early Wins
- COM-B Model and OWASP SECUR-E: Capability, Opportunity and Motivation Barriers

Day 3: Champion Core Knowledge and Incident First Response

- Coaching Notes on Phishing Cues, Pretexting and Baiting Tactics
- Coaching Colleagues on Passphrases, Password Managers and Multi-Factor Authentication
- Data Handling Coaching: Classification Labels, Sharing Links and Secure Disposal
- Device Security Checkpoints for Laptops, Phones and Removable Media
- Suspected Incident First Response: Triage Questions, Evidence Preservation and Escalation Paths

Day 4: Local Campaigns, Influence, Product Teams and Impact Measurement

- Local Awareness Campaign Toolkit: Lunch-and-Learns, Desk Drops and Micro-Challenges
- Influence Techniques for Peer-to-Peer Security Conversations and Resistant Colleagues
- Champions in Software and Product Teams: Threat Modelling Prompts and Secure Code Review Checklists
- Champion Impact Metrics: Phishing Report Rate, Engagement Logs and Culture Pulse Surveys
- Network Sustainment: Champion Fatigue, Turnover, Recognition Schemes and Community of Practice

Day 5: Case Work: Champions Network Design and Local Awareness Plan

- Case Business Unit Brief: Workforce Profile, Risk Hotspots and Stakeholder Map
- Case Network Design: Champion Coverage Map, Role Charter and Escalation Routes
- Case Local Awareness Plan: Campaign Themes, Messages, Channels and Success Measures
- Case Incident Walkthrough: Champion, Colleague and Security Team Hand-Offs
- Champions Network Design and Local Awareness Plan Presentation and Peer Challenge

Skills You Will Gain:

- Champion Network Design
- Champion Recruitment and Onboarding
- Peer Security Coaching
- Incident Triage and Escalation
- Awareness Campaign Planning
- Behavioural Barrier Diagnosis
- Security Culture Measurement
- Stakeholder Influence

Why Attend This Course:

- Leave with a Champions Network Design and Local Awareness Plan for a case business unit, ready to adapt to your own organisation
- Give champions a written charter and expectations that managers endorse, so the role survives busy periods
- Turn scattered security questions and near misses into routed reports that reach the security team quickly
- Compare champion practice with awareness leads, IT support staff and product teams from finance, energy, health and public service work

Conclusion:

A champions network works when the role is clear, champions are chosen and supported deliberately, and their effect on behaviour is measured. The course moves from the purpose and models of a champions network, through role charters, recruitment, onboarding and behaviour models, to the core knowledge champions pass on and first response to incidents, then local campaigns, influence, product team practice, impact metrics and sustainment. The final day produces a Champions Network Design and Local Awareness Plan for a case business unit.