CORE CONCEPT

Cybersecurity Awareness for Executives: Cyber Threats, Oversight and Crisis Decisions

CORE CONCEPT

Cybersecurity Awareness for Executives: Cyber Threats, Oversight and Crisis Decisions

Technical depth: Conceptual · **Practical mode:** Simulation

Introduction

Attackers increasingly target senior leaders directly, through impersonated payment requests, deepfake calls and compromised personal devices, and a cyber incident quickly becomes a leadership crisis with legal, financial and reputational consequences. Many executives still treat cybersecurity as a technical matter and meet their first real decision during an attack. This Core Concept course builds the awareness and judgement leaders need to protect themselves, question security reporting and act under pressure. Participants rehearse decisions in timed simulations and leave with an Executive Cyber Readiness Action Plan.

Course Objectives

- Recognise the attack patterns most likely to target leaders and the organisation, from ransomware to deepfake-enabled fraud
- Interpret NIST CSF 2.0, ISO/IEC 27001 and ISO/IEC 27014 well enough to question security leaders and judge their reports
- Apply personal security practices and verification protocols that protect executive accounts, devices and approvals
- Challenge management reporting on cyber risk, risk appetite and third-party exposure with informed questions
- Make and communicate time-critical decisions during a cyber incident within an agreed crisis structure
- Commit to an Executive Cyber Readiness Action Plan for personal and organisational follow-up

Target Audience

- Chief executives and general managers accountable for enterprise risk
- Board and audit committee members overseeing cyber risk
- Chief financial officers responsible for payment controls and cyber insurance
- Heads of legal, compliance and corporate communications who act in a cyber crisis
- Chief operating officers and business unit heads whose services depend on digital systems
- Senior public sector leaders accountable for citizen-facing services

CORE CONCEPT

Course Outline

Day 1: The Threat Landscape Facing Leaders

- Threat Actor Types and Motivations Illustrated with MITRE ATT&CK
- Ransomware and Double Extortion Business Models
- Business Email Compromise and Executive Impersonation Patterns
- Deepfake Voice and Video Fraud Targeting Senior Leaders
- Organisational Cyber Exposure Snapshot Using NIST CSF 2.0 Profiles

Day 2: Frameworks Every Executive Should Recognise

- NIST CSF 2.0 Govern Function and Leadership Responsibilities
- ISO/IEC 27001:2022 Information Security Management System Essentials
- ISO/IEC 27014 Governance of Information Security Processes
- NACD-ISA Cyber-Risk Oversight Principles for Boards
- Cyber Risk Quantification Concepts with the FAIR Model

Day 3: Leadership Behaviours and Oversight Questions

- Executive Personal Security: Devices, Travel and Social Media Footprint
- Payment and Approval Verification Protocols Against Impersonation
- Cybersecurity Dashboard and KPI Questions for Management Reports
- Cyber Risk Appetite Statement Principles
- Third-Party and Supply Chain Cyber Risk Questions for Suppliers

Day 4: Incidents, Crisis Decisions and Resilience

- Incident Management Lifecycle per ISO/IEC 27035-1
- Ransom Payment Decision Considerations and the Role of Legal Counsel
- Crisis Communication Protocol for Regulators, Customers and Media
- Recovery Objectives and Continuity Linkage with ISO 22301
- Executive Missteps Drawn from Published Breach Reviews

Day 5: Tabletop Simulation and Action Planning

- Ransomware Tabletop Simulation: The First Four Hours
- Deepfake Executive Fraud Simulation: Payment Approval Under Pressure
- Simulation Debrief and Decision Log Review
- Executive Cyber Readiness Action Plan Drafting
- Peer Review of Action Plans and Board Briefing Rehearsal

Skills You Will Gain

- Cyber Threat Awareness
- Cyber Risk Oversight
- Social Engineering Recognition
- Crisis Decision-Making
- Cyber Crisis Communication
- Security Report Interpretation
- Third-Party Risk Questioning
- Resilience Planning

Why Attend This Course

- Return to work with an Executive Cyber Readiness Action Plan tested in ransomware and deepfake fraud simulations
- Know which decisions fall to you in the first hours of an incident and who needs to be beside you
- Close the gaps in your own devices, accounts and approval habits that attackers use to reach the organisation
- Hear how leaders from other sectors and countries have handled breaches and what they would change

Conclusion

Cybersecurity is decided as much in the boardroom and the executive office as in the security operations centre. This course moves from the threats that target leaders, through the frameworks executives need to recognise and the oversight questions they should ask, to the decisions that shape the first hours of a crisis. The final day places participants inside timed simulations and turns the lessons into an Executive Cyber Readiness Action Plan, so that the next attempt on the organisation meets a prepared leadership team.