Updated on 22/08/2025

Sign up

Training Cybersecurity issues in your organization - for managers

3 days (21 hours)

Presentation

Our training course on the challenges of cybersecurity in your organization is specifically designed for executives, managers and IT managers, to give them a clear, strategic and pragmatic vision of cyber risks.

You'll discover how to take ownership of the strategic challenges of digital security within your organization.

The course covers both risk management and regulatory aspects, and includes practical workshops based on real-life scenarios.

At the end of the course, you'll be able to identify strategic threats to your organization, define a concrete action plan and reinforce the cyber culture within your teams.

Like all our training courses, this one is based on the latest regulatory and technological developments in cybersecurity, with a practical, operational approach.

Objectives

- Understand the strategic challenges of cybersecurity within an organization
- Situate cybersecurity within corporate governance and adapt your posture
- Understand the regulatory framework and legal obligations
- Foster a cyber culture within the company

Target audience

- Company managers
- Company executives
- IT managers

Prerequisites

- No prerequisites

Program of our training course The challenges of cybersecurity for your organization

[Day 1 - Morning]

Overview of threats and business impacts

- Evolving threats: ransomware, supply chain, fraud, social engineering
- Identifying critical assets and attack surface
- Economic, legal and reputational impacts: direct/indirect costs
- Examples of targeted vs. opportunistic attacks (SMEs / major accounts)
- Reading a business-oriented risk scenario
- Practical workshop: rapid analysis of a typical incident and impact assessment.

Governance, roles and responsibilities

- Aligning cyber strategy with corporate strategy
- Roles of COMEX, CIO, CISO, business lines and service providers
- Policies, charters and security committees
- Security culture: raising awareness and setting an example
- Budget, arbitration and prioritization

[Day 1 - Afternoon]

Regulations and standards (NIS2, RGPD, ISO 27001, NIST CSF)

- Scope and key obligations of NIS2 for the sectors concerned
- RGPD/security articulation: register, DPO, data breach
- ISO/IEC 27001 (ISMS) approach and controls
- NIST CSF 2.0 framework: organizing and measuring posture
- Pragmatic compliance roadmap

Risk management and investment prioritization

- Identifying, assessing and managing risks (mapping & heatmap)
- False invoice fraud: Business Email Compromise (BEC)
- Essential controls: IAM, patching, backups, EDR, MFA
- Zero Trust approach and segmentation
- Cyber insurance: guarantees, exclusions, requirements
- Practical workshop: Prioritizing an action plan within a limited budget.

[Day 2 - Morning]

Crisis management and business continuity (PCA/PRA)

- Alert chain and empowering players: establishing common reflexes in the face of an incident
- Real-life scenarios: ransomware, data leakage, denial of service, with everyone's role in the response
- Continuity and recovery plan (RTO/RPO) as a collective tool, not just a technical one
- Crisis communication: transparency and consistency to preserve trust (authorities, partners, customers, media)
- Strategic partners (insurers, IR/DFIR service providers): develop a relationship of trust before the crisis
- Practical workshop: Cyber crisis simulation. Role-playing of a COMEX faced with an attack and the leadership posture adopted, with a focus on decision-making, communication and collective management.

Developing a shared culture of cybersecurity

- Exemplarity and commitment of top management as a lever for cultural dissemination
- Differentiated awareness-raising: COMEX, managers, employees, partners
- Regular internal communication: campaigns, rituals, cybersecurity days, incident storytelling, etc.
- Integration into business practices: "security by design" and cultural indicators in projects
- Valuing and recognizing: encouraging best practices and incident reporting
- Practical workshop: Co-creation of a cyber management charter. In groups, define 5 concrete commitments that managers will make to their teams.

Companies concerned

This training course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced IT technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire enabling us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the forthcoming course, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or internal security difficulties (intra-company or virtual classroom) that could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Certification

A certificate will be awarded to each trainee who has completed the entire course.