

Updated on 01/23/2026

Register

# Training Cybersecurity challenges in your organization - for executives

1.5 days (10:30 a.m.)

## Presentation

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

You will discover how to address the strategic challenges of digital security in your organization.

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

By the end of this course, you will be able to identify strategic threats to your organization, define a concrete action plan, and strengthen the cyber culture within your teams.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

## Objectives

- Understand the strategic challenges of cybersecurity in an organization
- Position cybersecurity within corporate governance and adapt your approach
- Be familiar with the regulatory framework and legal obligations
- Promote a cyber culture within the company

# Target audience

- Business leaders
- Corporate executives
- IT managers

# Prerequisites

- No prerequisites

# Our training program Cybersecurity challenges within your organization

[Day 1 - Morning]

## Overview of threats and business impacts

- Evolution of threats: ransomware, supply chain, fraud, social engineering
- Identifying critical assets and attack surfaces
- Economic, legal, and reputational impacts: direct/indirect costs
- Examples of targeted vs. opportunistic attacks (SMEs/large 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 the executive committee, CIO, CISO, business units, and service providers
- Policies, charters, and security committee
- Security culture: awareness and exemplary management
- Budget, trade-offs, and prioritization

[Day 1 - Afternoon]

## Regulations and standards (NIS2, GDPR, ISO 27001, NIST CSF)

- Scope and key obligations of NIS2 for the sectors concerned
- GDPR/security coordination: register, DPO, data breaches
- 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 addressing risks (mapping & heatmap)
- False invoice fraud: Business Email Compromise (BEC)
- Essential controls: IAM, patching, backups, EDR, MFA
- Zero Trust approach and segmentation
- Cyber insurance: coverage, exclusions, requirements
- Hands-on workshop: Prioritizing an action plan with a limited budget.

### [Day 2 - Morning]

## Crisis management and business continuity (BCP/DRP)

- Alert chain and accountability of stakeholders: establishing common responses to incidents
- Real-life scenarios: ransomware, data leaks, denial of service, with each person'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 maintain trust (authorities, partners, customers, media)
- Strategic partners (insurers, IR/DFIR providers): develop a relationship of trust before the crisis
- Practical workshop: Cyber crisis simulation. Role-playing scenario of an executive committee facing an attack and the leadership stance adopted, with a focus on decision-making, communication, and collective management.

## Developing a shared culture of cybersecurity

- Exemplary behavior and commitment from top management as a lever for cultural diffusion
- Differentiated awareness: executive committee, managers, employees, partners
- Regular internal communication: campaigns, rituals, cybersecurity days, incident storytelling
- Integration into business practices: "security by design" and cultural indicators in projects
- Recognition and reward: encouraging best practices and incident reporting
- Practical workshop: Co-creation of a cyber management charter. Working in groups, define five concrete commitments that managers will communicate to their teams.

## Companies concerned

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

## Positioning at the start of training

The positioning at the start of the training complies with Qualiopi quality criteria. Upon

final registration, learners receive a self-assessment questionnaire that allows us to assess their estimated level of proficiency in different types of technologies, as well as their expectations and personal objectives for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could be problematic for the monitoring and smooth running of the training session.

## Teaching methods

Practical training: 60% practical, 40% theory. Training materials distributed in digital format to all participants.

## Organization

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

## Assessment

At the end of the session, a multiple-choice questionnaire is used to verify that the skills have been correctly acquired.

## Certification

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