BLACKBIRD FOR TRAINING

Cybersecurity Risk Management for Executives

17 – 21 May 2027
Lyon (France)



Cybersecurity Risk Management for Executives

Ref: 3255279_201685 **Date:** 17 – 21 May 2027 **Location:** Lyon (France) **Fees:** 5900 GBP

Introduction

In today's hyper-connected business environment, Cybersecurity Risk Management has become a strategic imperative for executives and decision-makers. Cyber threats are no longer just technical challenges—they are business risks that directly impact reputation, finances, and operational continuity. Every digital initiative, from cloud adoption to automation, introduces new vulnerabilities that must be managed proactively at the leadership level.

This course equips executives and senior leaders with the knowledge and frameworks necessary to understand, assess, and manage cybersecurity risks across their organizations. It bridges the gap between technical teams and executive decision-making, ensuring that cybersecurity becomes an integrated part of corporate governance, not just an IT function.

Participants will gain a strategic perspective on cyber risk, learning how to identify potential threats, evaluate their business impact, and implement governance models that foster resilience, accountability, and long-term protection of organizational assets.

Course Objectives

By the end of this course, participants will be able to:

- Understand the fundamentals and frameworks of cybersecurity risk management.
- Identify, assess, and prioritize cybersecurity risks within an organizational context.
- Integrate risk management practices into business strategy and executive decision-making.
- Develop governance structures that align cybersecurity with corporate objectives.
- Evaluate the financial and operational impact of cyber incidents.
- Oversee the creation and implementation of incident response plans.
- Strengthen communication between leadership, technical, and risk management teams.
- Ensure compliance with global cybersecurity standards and regulations.



Course Outlines

Day 1: Introduction to Cybersecurity and Risk Management

- Overview of cybersecurity and its importance for business continuity.
- The executive's role in cybersecurity governance.
- The lifecycle of risk management: identification, assessment, mitigation, and monitoring.
- Understanding emerging cyber threats and their implications.
- Building a strong risk-aware organizational culture.

Day 2: Identifying and Assessing Cyber Risks

- Techniques for recognizing cyber threats and vulnerabilities.
- Qualitative and quantitative risk assessment models.
- Using data-driven tools for evaluating risk exposure.
- Prioritizing risks based on business impact and likelihood.
- Case studies of real-world executive-level risk assessments.

Day 3: Building and Implementing Risk Management Strategies

- Designing an integrated cybersecurity risk management framework.
- Aligning cybersecurity strategies with business objectives.
- Developing risk mitigation plans and control mechanisms.
- Managing third-party and supply chain risks.
- Coordinating with internal stakeholders for policy execution.

Day 4: Governance, Compliance, and Incident Management

- The role of governance in establishing cybersecurity accountability.
- Overview of international standards: ISO 27001, NIST, GDPR, and others.
- Overseeing incident response planning and crisis communication.
- Executive leadership during cyber crises and reputational threats.
- Conducting post-incident reviews and compliance audits.

Day 5: Building a Cyber-Resilient Organization

- Embedding cybersecurity into organizational strategy.
- Establishing continuous improvement and monitoring programs.
- Fostering security awareness across all employee levels.
- Evaluating and benchmarking cybersecurity maturity.
- Creating a culture of shared responsibility for cyber risk.



Why Attend this Course: Wins & Losses!

- Gain a holistic understanding of cybersecurity risk from a leadership perspective.
- Improve strategic decision-making through informed risk evaluation.
- Learn how to align cybersecurity with the overall business strategy.
- Strengthen collaboration between technical teams and executive leadership.
- Develop governance frameworks that enhance organizational resilience.
- Ensure compliance with evolving cybersecurity standards and laws.
- Reduce financial and operational losses resulting from cyber incidents.
- Build a proactive culture of cybersecurity awareness within your organization.

Conclusion

The Cybersecurity Risk Management for Executives course empowers leaders to confidently navigate today's digital risk landscape. It goes beyond technical awareness to focus on strategic decision-making, governance, and long-term resilience.

Through a blend of practical frameworks, real-world examples, and executive-level insights, participants will learn how to anticipate, mitigate, and respond to cyber risks effectively. The course provides the tools and knowledge required to integrate cybersecurity into the fabric of organizational strategy and leadership.

In a world where digital threats evolve daily, executives who understand and manage cyber risk effectively gain a decisive advantage—protecting not only their data but also their brand, reputation, and stakeholders' trust.

