

Cybersecurity Essentials for Executives

Risk, strategy, incident preparedness and investment decisions

FA-0782 · 1 day (approximately 6–8 hours)

Cybersecurity

Introduction

Understand cybersecurity risks and the executive decisions needed to protect business assets and support an effective security programme. Explore practical scenarios, leadership responsibilities, incident preparation and investment trade-offs. The course is an executive foundation, not a technical audit or assurance of compliance.

Learning outcomes

- Recognise common threats, insider risks and relevant vulnerabilities for discussion with technical teams.
- Align cybersecurity priorities, accountability and culture with business objectives.
- Evaluate authentication, data protection, network, remote-work and cloud practices at a leadership level.
- Outline executive communication, escalation and decision-making roles during an incident.
- Identify jurisdiction-specific legal obligations requiring qualified review.
- Evaluate cybersecurity investments and communicate risk/value trade-offs.

Prerequisites

- Basic familiarity with information technology and computer systems.
- General understanding of the role of technology in business operations.

- No prior knowledge of cybersecurity is required, as the course will cover essential concepts from the ground up.

Access to a computer and course materials.

Training outline

1. Module 1 – Cybersecurity landscape

- Introduction to cybersecurity: Definitions, importance, and potential consequences of cyberattacks.
- Cybersecurity challenges in the digital age: The evolving threat landscape and common attack vectors.
- Key cybersecurity terminologies and concepts.

2. Module 2 – Risks and vulnerabilities

- Recognizing common cybersecurity threats: Phishing, ransomware, social engineering, etc.
- Understanding insider threats and the human element in cybersecurity.
- Assessing vulnerabilities in technology, networks, and infrastructure.

3. Module 3 – Leadership strategy

- Establishing a cybersecurity culture within the organization.
- Role of executives in promoting cybersecurity awareness and accountability.
- Integrating cybersecurity into business operations and decision-making processes.

4. Module 4 – Security practices

- Secure password management and authentication methods.
- Data protection and encryption techniques.
- Network security and segmentation.
- Secure remote work practices.
- Security in the cloud environment.

5. Module 5 – Incident and crisis preparedness

- Preparing for cybersecurity incidents: Incident response planning.
- Executives' role during a cyber incident: Communication, decision-making, and escalation.
- Engaging with cybersecurity experts and law enforcement during an incident.

6. Module 6 — Compliance and legal context

- Understanding relevant cybersecurity regulations and industry standards.
- Navigating legal implications of data breaches and cyber incidents.
- The importance of transparency and disclosure in case of a data breach.

Applicable requirements and disclosure obligations depend on jurisdiction, sector and incident circumstances; obtain qualified legal advice for decisions.

7. Module 7 — Investment and value

- Evaluating cybersecurity investment: Balancing cost and risk.
- Communicating the value of cybersecurity to stakeholders.
- Potential value and limitations of security-investment estimates.

Learning approach

Interactive presentations, case studies, group discussions and scenario-based exercises connect security decisions to business responsibilities.