

Cybersecurity for Leadership in Air Cargo & Logistics

Secure Your Operations. Protect Your People. Lead with Confidence.

AVIATION NOW
ACADEMY



1 DAY WORKSHOP | MIN PARTICIPANTS | Available Languages: DE+EN

AIR CARGO COMPLIANCE

AVIATIONNOW.ACADEMY

Description

The Cybersecurity Leadership Program is an intensive one-day workshop specifically designed for senior leaders and executives in air cargo and logistics organizations. In an industry where a single cyberattack can halt cargo systems, ground flights, and expose your organization to regulatory penalties, cybersecurity is no longer a technical detail – it is a board-level business priority.

This program gives leaders a practical, grounded understanding of the cyber threat landscape specific to logistics and aviation – including ransomware, supply chain breaches, phishing, insider threats, and OT/IoT vulnerabilities. Participants will explore real-world case studies, assess compliance obligations across ICAO, TSA, GDPR, and ISO 27001, and develop a concrete crisis response posture for their organization. By the end of the workshop, participants will have co-created an organizational cybersecurity resilience roadmap and leave with tangible tools. No prior knowledge of AI is required. The workshop is designed to be accessible for all levels of technical familiarity while remaining strategically substantive for experienced leaders.

Target group

- Leadership and senior management in air cargo and logistics organizations
- C-Suite executives (CEO, COO, CTO, CDO) at airlines, cargo carriers, and logistics hubs
- VP-level and Director-level leaders in cargo, operations, IT, compliance, and digital transformation
- Senior managers at ground handling companies, freight forwarders and cargo terminal operators
- Leaders accountable for operational continuity, regulatory compliance, and cyber risk governance
- Professionals responsible for vendor management, data protection, and incident response planning

Class location: Virtual workshop (Classroom training in-company on request)

Included: Presentation materials (PDF), sector-specific cyber threat briefing, compliance & regulatory overview, interactive group exercises, digital participant workbook, certificate
This course is delivered in collaboration with AITHEA GmbH.

Learning objectives

- Understand the current cyber threat landscape and its implications for air cargo and logistics operations.
- Identify the operational, financial, regulatory, and reputational impacts of cyber incidents.
- Recognize and assess key cyber threats, including ransomware, phishing, supply chain attacks, insider threats, and OT/IoT vulnerabilities.
- Understand the regulatory and compliance landscape, including ICAO Cybersecurity Framework, TSA Security Directives, GDPR, ISO 27001, and relevant cybersecurity governance requirements.
- Apply cybersecurity risk management principles to strengthen organizational resilience and operational continuity.
- Assess organizational cybersecurity readiness and identify critical vulnerabilities and capability gaps.
- Develop effective cyber governance structures, vendor assessment processes, and risk management frameworks.
- Design and communicate an appropriate cyber incident response posture for leadership and operational teams.
- Understand the risks associated with Shadow IT, insider threats, and emerging technology adoption.
- Strengthen staff awareness and promote a culture of cybersecurity responsibility across the organization.
- Evaluate cyber insurance readiness and understand risk reduction expectations from insurers.
- Lead cybersecurity strategy and resilience initiatives aligned with organizational objectives and regulatory obligations.

Course outcomes

- A leadership-level understanding of the cyber threats, risks, and regulatory obligations affecting air cargo and logistics operations.
- The ability to assess organizational cybersecurity readiness, priorities risks, and strengthen resilience across operations.
- A practical Cybersecurity Resilience Roadmap and the confidence to lead cybersecurity governance, awareness, and risk management initiatives within their organization.



AITHEA

