Training Course on Cybersecurity for Airport Executives

Professional Development Training Course Outline

Category	Aviation and Airport Management	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In an era of escalating digital threats, **cybersecurity resilience** is paramount for the global aviation industry. Airports, as critical national infrastructure and interconnected hubs, face sophisticated **cyber-attacks** that can disrupt operations, compromise sensitive data, and threaten passenger safety. Training Course on Cybersecurity for Airport Executives is meticulously designed to equip senior leaders with the strategic understanding and practical **risk management** frameworks necessary to navigate this complex **threat landscape**. It emphasizes a holistic approach to **aviation cybersecurity**, integrating **governance, risk, and compliance (GRC)** principles with cutting-edge **security technologies** to build an **incident response** ready organization.

This program goes beyond technical jargon, focusing on the executive's role in fostering a robust **cybersecurity culture** and making informed decisions that protect **critical airport systems** and **passenger data privacy**. By understanding the latest **cyber threat intelligence** and **regulatory frameworks**, airport executives will be empowered to implement proactive **cyber defense strategies**, enhance **operational continuity**, and ensure **business resilience** against persistent and evolving **cyber risks**. The course provides actionable insights into developing comprehensive **cybersecurity policies**, **incident management plans**, and fostering cross-organizational collaboration to build a truly **secure aviation ecosystem**.

Programme Curriculum

Training Course on Cybersecurity for Airport Executives

Introduction

In an era of escalating digital threats, **cybersecurity resilience** is paramount for the global aviation industry. Airports, as critical national infrastructure and interconnected hubs, face sophisticated **cyber-attacks** that can

disrupt operations, compromise sensitive data, and threaten passenger safety. Training Course on Cybersecurity for Airport Executives is meticulously designed to equip senior leaders with the strategic understanding and practical **risk management** frameworks necessary to navigate this complex **threat landscape**. It emphasizes a holistic approach to **aviation cybersecurity**, integrating **governance, risk, and compliance (GRC)** principles with cutting-edge **security technologies** to build an **incident response** ready organization.

This program goes beyond technical jargon, focusing on the executive's role in fostering a robust **cybersecurity culture** and making informed decisions that protect **critical airport systems** and **passenger data privacy**. By understanding the latest **cyber threat intelligence** and **regulatory frameworks**, airport executives will be empowered to implement proactive **cyber defense strategies**, enhance **operational continuity**, and ensure **business resilience** against persistent and evolving **cyber risks**. The course provides actionable insights into developing comprehensive **cybersecurity policies**, **incident management plans**, and fostering cross-organizational collaboration to build a truly **secure aviation ecosystem**.

Course Duration

10 days

Course Objectives

1. Develop advanced leadership skills to champion and embed cybersecurity as a core strategic imperative across airport operations.
2. Implement robust, **risk-based cybersecurity frameworks** aligned with international standards (e.g., NIST, ISO 27001) for comprehensive **threat mitigation**.
3. Master the identification and analysis of **aviation-specific cyber threats**, including **APT groups**, **ransomware**, and **supply chain vulnerabilities**.
4. Establish effective **cybersecurity governance** structures and ensure adherence to evolving **regulatory mandates** (e.g., ICAO, GDPR, FAA).
5. Develop strategies for protecting **operational technology (OT)** and **industrial control systems (ICS)** within airport environments.
6. Formulate comprehensive **incident response plans** and conduct **tabletop exercises** to enhance **cyber crisis management** capabilities.
7. Guide the secure adoption of emerging technologies like **AI, IoT, and Cloud Computing** within airport infrastructure.
8. Implement stringent **data privacy** and **data protection** measures for sensitive passenger and operational data.
9. Foster a proactive and vigilant **cybersecurity culture** across all levels of the airport organization.
10. Develop robust processes for managing **third-party cybersecurity risks** associated with vendors and partners.
11. Ensure **cyber resilience** and **business continuity** through effective disaster recovery and contingency planning.
12. Strategically evaluate and prioritize investments in **next-generation cybersecurity solutions**.
13. Understand methodologies for **threat hunting** and implementing proactive **cyber defense** mechanisms.

Organizational Benefits

- Minimize disruption from cyberattacks, ensuring seamless airport operations and passenger flow.
- Mitigate the financial impact of breaches and protect the airport's public image and stakeholder trust.

- Ensure adherence to national and international aviation cybersecurity regulations, avoiding costly fines and legal repercussions.
- Develop a proactive and adaptive approach to identifying, assessing, and mitigating cyber risks.
- Cultivate a workforce that is aware, vigilant, and actively contributes to the airport's overall security posture.
- Make informed decisions on cybersecurity investments, maximizing the return on security spending.
- Demonstrate a commitment to passenger safety and data privacy, boosting public trust in air travel.
- Position the airport as a leader in aviation security, attracting airlines and partners.

Target Audience

1. Airport Directors and CEOs
2. Chief Information Officers (CIOs) and IT Directors.
3. Chief Security Officers (CSOs) and Aviation Security Managers.
4. Operations Managers.
5. Legal and Compliance Officers.
6. Heads of Air Traffic Control (ATC) and Air Navigation Service Providers (ANSP) Management
7. Emergency Management and Business Continuity Planners.
8. Airport Board Members and Senior Executives

Course Outline

Module 1: The Evolving Aviation Cyber Threat Landscape

- Understanding the unique vulnerabilities of airport ecosystems (airside, landside, IT, OT systems).
- Analysis of current and emerging cyber threats targeting aviation (ransomware, phishing, state-sponsored attacks).
- Impact assessment of cyber incidents on airport operations, safety, and reputation.
- **Case Study**: The NotPetya attack's impact on Maersk and its implications for interconnected global logistics, drawing parallels to airport systems.
- **Case Study**: Analysis of a significant airport data breach (e.g., SITA Passenger Service System incident) and its consequences.

Module 2: Cybersecurity Governance, Risk, and Compliance (GRC) for Airports

- Establishing a robust cybersecurity governance framework within the airport organizational structure.
- Implementing risk assessment methodologies tailored for aviation environments.
- Navigating international and national aviation cybersecurity regulations (ICAO Annex 17, EU Regulations, TSA Directives).
- **Case Study**: A successful airport's journey to ISO 27001 certification and its impact on security posture.
- **Case Study**: Regulatory non-compliance case study and the resulting fines/reputational damage for an airport.

Module 3: Protecting Critical Airport Infrastructure and Operational Technology (OT)

- Understanding the convergence of IT and OT in airports and its cybersecurity implications.
- Securing Air Traffic Management (ATM) systems, baggage handling systems, and ground support equipment.
- Implementing segmentation and access controls for critical operational networks.
- **Case Study**: A simulated cyberattack scenario on an airport's baggage handling system and the coordinated response.

- **Case Study**: Best practices in securing SCADA/ICS systems in a major international airport.

Module 4: Incident Response and Crisis Management in Aviation

- Developing a comprehensive incident response plan tailored for aviation cyber incidents.
- Establishing an effective Cyber Security Operations Center (CSOC) or leveraging external capabilities.
- Techniques for containment, eradication, and recovery from cyberattacks.
- **Case Study**: Post-mortem analysis of a real-world airport cyber incident (anonymized) focusing on lessons learned in incident response.
- **Case Study**: A tabletop exercise simulating a ransomware attack on airport IT systems, evaluating executive decision-making.

Module 5: Data Privacy and Passenger Information Protection

- Understanding data privacy regulations (GDPR, CCPA, etc.) and their applicability to airport data.
- Implementing data encryption, anonymization, and access control for sensitive passenger data.
- Managing data breaches involving passenger information and regulatory notification requirements.
- **Case Study**: Analysis of a breach involving passenger Personally Identifiable Information (PII) at an airline or airport, focusing on mitigation and communication.
- **Case Study**: Best practices for implementing privacy-by-design principles in new airport digital initiatives.

Module 6: Supply Chain Cybersecurity Risk Management

- Identifying and assessing cybersecurity risks introduced by third-party vendors and partners.
- Developing robust vendor security assessment and management programs.
- Contractual clauses and due diligence for ensuring supply chain cybersecurity.
- **Case Study**: A supply chain attack impacting an airport's IT services, demonstrating the ripple effect of vendor vulnerabilities.
- **Case Study**: Implementing a successful third-party risk management framework at an airport, showcasing measurable improvements.

Module 7: Cybersecurity Culture and Human Factors

- The role of human error in cybersecurity incidents and strategies for mitigation.
- Developing effective security awareness training programs for all airport staff.
- Fostering a "security-first" mindset from the executive suite to frontline employees.
- **Case Study**: A successful security awareness campaign at an airport that significantly reduced phishing click-through rates.
- **Case Study**: Analyzing an insider threat incident (accidental or malicious) and the preventative measures that could have been in place.

Module 8: Emerging Technologies and Future Cybersecurity Challenges

- Cybersecurity implications of AI, IoT, 5G, and blockchain adoption in airports.
- Securing connected aircraft and ground-to-air communication systems.
- Preparing for quantum computing threats and future cryptographic needs.
- **Case Study**: Examining the cybersecurity challenges and mitigation strategies for a fully automated baggage handling system utilizing IoT devices.
- **Case Study**: Discussion on the potential cybersecurity risks and benefits of AI-powered surveillance systems in airports.

Module 9: Threat Hunting and Proactive Cyber Defense

- Understanding the principles of threat hunting and proactive threat detection.
- Leveraging threat intelligence platforms and security information and event management (SIEM) systems.
- Implementing endpoint detection and response (EDR) and network detection and response (NDR) solutions.
- **Case Study**: An airport's successful implementation of a threat hunting program that identified and neutralized a persistent threat.
- **Case Study**: Utilizing a Security Orchestration, Automation, and Response (SOAR) platform to improve response times to identified threats.

Module 10: Cloud Security in Airport Operations

- Securing airport data and applications hosted in cloud environments (public, private, hybrid).
- Understanding shared responsibility models in cloud security.
- Implementing cloud access security brokers (CASB) and secure cloud configurations.
- **Case Study**: Migrating a critical airport application to the cloud securely, outlining the challenges and solutions.
- **Case Study**: A cloud misconfiguration leading to a security vulnerability at an organization (not necessarily airport, but relevant lessons).

Module 11: Application Security and Secure Development Lifecycle

- Ensuring the security of custom-built and third-party applications used in airport operations.
- Integrating security into the software development lifecycle (SDLC).
- Addressing common application vulnerabilities (e.g., OWASP Top 10) in airport systems.
- **Case Study**: An airport's experience in identifying and remediating critical vulnerabilities in a passenger-facing mobile application.
- **Case Study**: Implementing DevSecOps practices for an internal airport software development team.

Module 12: Business Continuity and Disaster Recovery Planning

- Developing comprehensive business continuity plans to maintain essential airport functions during a cyber crisis.
- Establishing robust data backup and recovery strategies.
- Conducting regular business continuity and disaster recovery drills.
- **Case Study**: An airport's successful recovery from a major IT system outage (cyber-related or otherwise) highlighting effective BCDR.
- **Case Study**: The importance of redundant systems and diversified data storage for maintaining operational continuity.

Module 13: Cybersecurity Metrics, Reporting, and Board Engagement

- Defining key performance indicators (KPIs) and metrics for cybersecurity effectiveness.
- Developing clear and concise cybersecurity reports for executive leadership and the board.
- Strategies for engaging the board in cybersecurity discussions and investment decisions.
- **Case Study**: A presentation of effective cybersecurity dashboards used by a leading airport to communicate risk to the board.
- **Case Study**: Analyzing how a proactive CISO successfully secured increased cybersecurity budget through effective communication with the board.

Module 14: Legal and Ethical Considerations in Cybersecurity

- Understanding legal implications of cyberattacks, data breaches, and regulatory non-compliance.
- Ethical considerations in cybersecurity practices, including data collection and surveillance.
- Cyber insurance: understanding coverage, limitations, and claims processes.
- **Case Study**: A legal challenge faced by an organization due to a data breach and the lessons learned in legal counsel engagement.
- **Case Study**: Debating the ethical implications of using advanced facial recognition technology for security purposes in airports.

Module 15: Future-Proofing Airport Cybersecurity

- Developing a long-term cybersecurity roadmap for the airport.
- Strategies for continuous improvement and adaptation to new threats.
- Building a network of cybersecurity partnerships (government, industry, academia).
- **Case Study**: A forward-thinking airport's multi-year cybersecurity investment strategy and its anticipated benefits.
- **Case Study**: The benefits of collaborative threat intelligence sharing between airports and government agencies.

Training Methodology

This course employs a dynamic and interactive training methodology designed for executive-level learning, combining:

- **Interactive Lectures and Presentations**: Engaging delivery of core concepts with emphasis on strategic implications.
- **Real-World Case Studies and Discussions**: In-depth analysis of actual cyber incidents and best practices from the aviation sector and beyond.
- **Tabletop Exercises and Simulations**: Hands-on scenarios to practice incident response, crisis management, and decision-making under pressure.
- **Group Activities and Collaborative Problem-Solving**: Fostering peer-to-peer learning and sharing of experiences.
- **Expert Panel Discussions**: Insights from leading cybersecurity professionals, aviation authorities, and industry veterans.
- **Q&A Sessions and Open Forums**: Opportunities for direct engagement with instructors and expert clarification.
- **Executive Briefings and Strategic Planning Workshops**: Focused sessions on developing actionable cybersecurity strategies for their respective airports.
- **Pre-reading Materials and Post-course Resources**: Supplemental content for continuous learning and reference.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com