Airport Information Systems and Cybersecurity Resilience Training Course

Ref: #AIR6377

Course Introduction / Overview:

The global aviation industry operates on a complex web of interconnected information systems, from passenger processing and baggage handling to air traffic control and ground operations. This digital transformation, while enhancing efficiency, also exposes airports to a sophisticated and evolving landscape of cyber threats. A single breach can cause catastrophic disruptions, financial loss, and reputational damage, compromising the safety and security of millions. This intensive training course provides a comprehensive framework for understanding and securing these critical infrastructures. Drawing on principles outlined by experts like Dr. Daniel J. Ragsdale in works such as "Cybersecurity in the Air Transportation System," the program delves into the unique vulnerabilities of Airport Operational Databases (AODB), Flight Information Display Systems (FIDS), and Operational Technology (OT). BIG BEN Training Center has designed this course to move beyond theoretical concepts, equipping participants with practical, actionable strategies for building a robust and resilient cybersecurity posture. Participants will learn to identify threats, implement effective controls, manage incidents, and ensure regulatory compliance, safeguarding the future of airport operations in an increasingly digital world.

Target Audience / This training course is suitable for:

- Airport IT and Cybersecurity Managers.
- Aviation Security Professionals.
- Airport Operations and Management Staff.
- Information Security Analysts and Consultants.
- Compliance and Risk Management Officers.
- Air Navigation Service Provider (ANSP) personnel.
- Engineers and Technicians managing airport systems.
- Government and Regulatory Agency Officials.

Target Sectors and Industries:

- Airport Authorities and Operators.
- Airlines.
- Ground Handling Service Providers.
- Air Navigation Service Providers (ANSPs).
- Aviation Technology and System Integrators.
- Government, Military, and Civil Aviation Authorities.
- Security and Risk Management Consultancies.

Target Organizations Departments:

- Information Technology (IT) and Information Security.
- Airport Operations and Airside Management.
- Corporate Security and Physical Security.
- Risk Management and Compliance.
- Engineering and Maintenance.
- Internal Audit and Governance.
- Emergency Response and Crisis Management.

Course Offerings:

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

- Analyze the unique architecture of airport information systems and their specific vulnerabilities.
- Evaluate the modern cyber threat landscape targeting the aviation sector.
- Implement cybersecurity frameworks and best practices such as NIST and ICAO guidelines.
- Develop a comprehensive risk management strategy for airport IT and OT environments.
- Design and deploy robust security controls for critical airport networks and applications.
- Formulate an effective cyber incident response and recovery plan tailored to airport operations.
- Ensure compliance with international and national aviation cybersecurity regulations.
- Assess and mitigate security risks associated with third-party vendors and the supply chain.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to foster a dynamic and immersive learning experience that bridges theory with real-world application. This course utilizes a blended approach, combining expert-led instruction with highly interactive modules. Participants will engage in detailed case study analyses of actual airport cyber incidents, deconstructing the attack vectors, response strategies, and lessons learned. Collaborative group workshops will challenge teams to develop risk assessments and incident response plans for simulated airport environments, promoting teamwork and practical problem-solving. Interactive sessions, Q&A panels, and peer-to-peer discussions are integrated throughout the five days to encourage knowledge sharing and address specific challenges faced by participants in their own organizations. The emphasis is on practical application, ensuring that attendees leave not just with knowledge, but with the confidence and skills to implement effective cybersecurity measures immediately upon their return to the workplace.

Course Agenda (Course Units):

Unit One: The Airport Digital Ecosystem and Threat Landscape

- Introduction to Airport Information Systems (AIS).
- Key Systems Explored: AODB, FIDS, BHS, CUPPS/CUTE.
- Understanding Operational Technology (OT) in Airports.
- The Convergence of IT and OT Environments.
- Mapping the Airport Attack Surface.
- Common Cyber Threats: Ransomware, DDoS, Phishing, Insider Threats.
- Case Studies of Major Aviation Cyber Incidents.

Unit Two: Cybersecurity Governance, Risk, and Compliance

- International and National Aviation Cybersecurity Regulations.
- Applying the NIST Cybersecurity Framework to Airports.
- ICAO Cybersecurity Guidelines and Standards.
- Conducting a Comprehensive Cybersecurity Risk Assessment.
- Developing an Airport Cybersecurity Governance Structure.
- Building a Robust Security Policy and Procedures Framework.
- Vendor and Supply Chain Risk Management.

Unit Three: Securing Airport Information and Operational Technology

- Network Segmentation and Access Control Strategies.
- Securing Airport Wi-Fi and Passenger-Facing Systems.
- Endpoint Detection and Response (EDR) for Airport Terminals.
- Protecting SCADA and Industrial Control Systems (ICS).
- Data Encryption and Protection for Sensitive Aviation Data.
- Identity and Access Management (IAM) Best Practices.
- Physical Security Integration with Cybersecurity Controls.

Unit Four: Threat Detection, Incident Response, and Recovery

- Building an Airport Security Operations Center (SOC).
- Implementing Security Information and Event Management (SIEM).
- Leveraging Threat Intelligence in the Aviation Sector.
- Developing a Cyber Incident Response Plan (IRP).
- Conducting Tabletop Exercises and Simulation Drills.
- Digital Forensics and Investigation in an Airport Context.
- Business Continuity and Disaster Recovery Planning.

Unit Five: Advanced Cybersecurity and Future Resilience

- Cloud Security for Airport Applications and Data Storage.
- Securing the Internet of Things (IoT) in a Smart Airport.
- The Role of Artificial Intelligence (AI) in Aviation Cybersecurity.
- Addressing the Human Factor: Security Awareness and Training.
- Building a Culture of Cybersecurity Across the Airport.
- Developing a Long-Term Cybersecurity Resilience Roadmap.
- The Future of Airport Cybersecurity and Emerging Threats.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

As airports increasingly adopt IoT and AI for operational efficiency, how does the traditional perimeter-based security model need to evolve to protect against new, interconnected threat vectors?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by focusing specifically on the critical intersection of Information Technology (IT) and Operational Technology (OT) within the unique airport environment, a convergence points often overlooked by general cybersecurity training. While other programs may cover broad security principles, this curriculum is meticulously tailored to address the specific systems, protocols, and regulatory pressures of the aviation industry. We move beyond theoretical frameworks to immerse participants in practical, scenario-based learning, using case studies drawn from real-world airport cyber incidents. The emphasis is on building holistic resilience, not just technical defense. Participants will learn to develop integrated strategies that encompass governance, risk management, incident response, and human factors, creating a robust security culture. The curriculum is designed to empower professionals to protect the entire airport ecosystem, from passenger data and flight information systems to baggage handling and airside control systems, ensuring a level of specialized expertise that is essential for safeguarding this critical global infrastructure.