Aviation Cybersecurity Risk and Resilience Management Training Course

Ref: #AVI5441

Course Introduction / Overview:

The aviation industry's increasing reliance on interconnected digital systems, from avionics and air traffic management to ground operations and passenger services, has created a complex and high-stakes cyber threat landscape. This training course provides a comprehensive exploration of aviation cybersecurity, focusing on proactive risk management and the development of robust resilience strategies. As detailed by experts like Dr. Marina Krotofil in the field of industrial control system security, the convergence of Information Technology (IT) and Operational Technology (OT) in aviation presents unique challenges that require specialized knowledge. This program, offered by BIG BEN Training Center, moves beyond generic cybersecurity principles to address the specific vulnerabilities, regulatory frameworks, and operational imperatives of the air transport ecosystem. Participants will delve into critical standards and guidance, such as those outlined in documents like DO-326A/ED-202A, learning to identify, assess, and mitigate cyber threats to aircraft, airports, and air navigation services. The curriculum is designed to equip professionals with the practical skills needed to build a security-first culture and ensure the safety, security, and continuity of aviation operations in the face of evolving cyber threats.

Target Audience / This training course is suitable for:

- Aviation Cybersecurity Analysts and Specialists.
- Airline and Airport IT and Security Managers.
- Air Traffic Management (ATM) and ANSP Personnel.
- Aircraft Systems and Avionics Engineers.
- Aviation Safety and Compliance Officers.
- Government and Civil Aviation Authority Regulators.
- Aviation Risk Management Professionals.
- Corporate Security and Operations Executives in the aviation sector.
- Pilots and Flight Operations Managers with an interest in cybersecurity.

Target Sectors and Industries:

- Commercial Airlines and Cargo Carriers.
- Airport Authorities and Operators.
- Air Navigation Service Providers (ANSPs).
- Aircraft and Avionics Manufacturers (OEMs).
- Maintenance, Repair, and Overhaul (MRO) Organizations.
- Aviation Supply Chain and Logistics Partners.
- Government, Military, and Civil Aviation Authorities.
- Aviation Insurance and Risk Management Firms.

Target Organizations Departments:

- Information Technology and Cybersecurity.
- Flight Operations and Control Centers.
- Safety and Regulatory Compliance.
- Engineering and Maintenance.
- Risk Management and Internal Audit.
- Corporate Security and Crisis Management.
- Airport Operations and Ground Handling.
- Executive and Senior Management.

Course Offerings:

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

- Develop a comprehensive understanding of the aviation-specific cyber threat landscape.
- Apply international standards and regulatory frameworks like DO-326A/ED-202A.
- Conduct thorough cybersecurity risk assessments for aircraft and ground systems.
- Design and implement security controls for both IT and OT environments in aviation.
- Create and test an effective aviation-focused cyber incident response plan.
- Analyze the security implications of connected aircraft and modern avionics.
- Evaluate and mitigate cybersecurity risks within the aviation supply chain.
- Foster a proactive cybersecurity culture within their organization.
- Integrate cybersecurity considerations into aviation safety management systems.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, practical, and highly interactive, ensuring participants can apply learned concepts directly to their professional roles. This course moves beyond traditional lectures by incorporating a blend of expert-led instruction, in-depth case study analysis of real-world aviation cyber incidents, and collaborative group exercises. Participants will engage in hands-on workshops focused on threat modeling for avionics systems and developing risk mitigation strategies for airport operational technology. Interactive sessions will facilitate peer-to-peer learning and the sharing of diverse industry perspectives. We will utilize simulation exercises where teams respond to a staged cyber-attack on an airline's operational systems, forcing them to make critical decisions under pressure. Continuous feedback from the instructor and a focus on practical problem-solving are central to the learning experience. This dynamic approach ensures that attendees not only grasp the theoretical frameworks of aviation cybersecurity but also develop the critical thinking and practical skills necessary to build and maintain a resilient aviation ecosystem.

Course Agenda (Course Units):

Unit One: The Aviation Cybersecurity Ecosystem

- Introduction to Aviation Digital Transformation.
- Unique Threats and Vulnerabilities in the Aviation Sector.
- Key Terminology: IT, OT, and Aviation-Specific Systems.
- The Interplay Between Cybersecurity and Aviation Safety.
- Overview of Global Regulatory Frameworks (ICAO, EASA, FAA).
- Understanding the Connected Aircraft Environment.
- Major Stakeholders and Their Security Responsibilities.

Unit Two: Aviation Cybersecurity Risk Management

- Foundations of Cybersecurity Risk Assessment.
- Applying NIST Cybersecurity Framework to Aviation.
- Deep Dive into DO-326A/ED-202A Airworthiness Security Process.
- Threat Modeling for Aircraft Systems and Networks.
- Vulnerability Assessment for Ground and Airport Systems.
- Conducting a Business Impact Analysis (BIA) for Airline Operations.
- Quantitative vs. Qualitative Risk Analysis in Aviation.

Unit Three: Securing Aviation Systems and Infrastructure

- Security Architecture for Aircraft Data Networks.
- Protecting Air Traffic Management (ATM) and CNS Systems.
- Cybersecurity for Airport Operational Technology (OT).
- Securing Passenger Processing and Data Systems.
- Implementing Identity and Access Management (IAM) Controls.
- Data Protection and Privacy in the Aviation Context.
- Physical Security as a Component of Cybersecurity.

Unit Four: Cyber Resilience and Incident Response

- Developing an Aviation-Specific Cyber Incident Response Plan (CIRP).
- Incident Detection, Triage, and Analysis Techniques.
- Crisis Communication Strategies for Cyber Events.
- Containment, Eradication, and Recovery Procedures.
- Business Continuity and Disaster Recovery Planning for Airlines.
- Forensic Readiness and Evidence Collection.
- Post-Incident Analysis and Lessons Learned.

Unit Five: Advanced Topics and Future Challenges

- Cybersecurity in the Aviation Supply Chain.
- The Human Factor: Insider Threats and Security Awareness Training.
- Security Implications of Unmanned Aircraft Systems (UAS/Drones).
- The Role of Artificial Intelligence (AI) in Aviation Cybersecurity.
- Threat Intelligence Sharing in the Aviation Community (ISACs).
- Preparing for Future Aviation Technologies (e.g., Urban Air Mobility).
- Building and Measuring a Mature Aviation Cybersecurity Program.

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 aviation systems become increasingly autonomous, how does the traditional model of risk ownership shift between manufacturers, operators, and regulators, and what new frameworks are needed to govern liability in the event of a cyber-induced failure?

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

This training course distinguishes itself by offering a holistic and deeply specialized perspective on aviation cybersecurity, moving far beyond generic IT security principles. Its primary uniqueness lies in its dedicated focus on the convergence of IT, Operational Technology (OT), and the specific airworthiness security standards that govern the industry, such as DO-326A/ED-202A. Unlike other programs that may treat aviation as just another sector, this course is built from the ground up around the unique operational imperatives and safety-critical nature of air transport. We emphasize practical, real-world application through case studies derived from actual aviation incidents and simulations that mirror the complex decision-making environment of an airline or airport operations center. Furthermore, the curriculum comprehensively addresses the entire aviation ecosystem, from the aircraft flight deck and supply chain to air traffic control and ground operations. It places significant emphasis on the human factor and building a resilient security culture, recognizing that technology alone is insufficient. The course provides a strategic-level understanding, enabling participants not just to implement controls, but to build and lead a mature, proactive, and adaptive cybersecurity program fit for the challenges of modern aviation.