SAFE SKIES.
SUSTAINABLE FUTURE.
A UNITED NATIONS SPECIALIZED AGENCY

भारतीय विमानपत्तन प्राधिकरण
AIRPORTS AUTHORITY OF INDIA

Holistic Risk Management in Aviation Cybersecurity

Ensuring a Holistic Approach Across Safety, Security, Efficiency, and Capacity

Dr Sharad Kumar

Member (Ops), Airports Authority of India

memberops@aai.aero

Aviation Cybersecurity: The Growing Threat Landscape

Statistics:

The aviation industry experienced a **131% increase in cyberattacks** between 2022 and 2023 (European Regions Airline Association, 2024).

85% of airlines have faced attempts to disrupt their systems (IATA, 2022).

The average cost of a data breach is **$4.88 million** per data breach incident (IBM, 2024).

Potential Cyber Threats:

Ransomware attacks on airport systems (e.g., Atlanta Airport, 2018).

GPS spoofing and jamming affecting flight navigation.

Unauthorized access to air traffic control and Airport Operations systems.

Distributed Denial of Service attack disrupting operational systems

The For Pillars of Holistic Aviation Risk Management

Safety: Ensuring passenger and crew safety through robust systems.

Security: Protecting against malicious cyber activities.

Efficiency: Maintaining operational performance and minimizing delays.

Capacity: Ensuring systems can handle growing air traffic demands.

Interdependence:

A cyber incident can compromise safety (e.g., tampering with flight systems).

At the same time, Cybersecurity measures must not hinder operational efficiency or capacity.

Interconnection between Cybersecurity and Safety

Key Link:

Cybersecurity directly impacts the safety of aviation operations by protecting critical systems from malicious interference.

Examples:

Flight Systems: A cyberattack on flight control systems could compromise aircraft safety.

Air Traffic Management (ATM): Disruption of ATM systems could lead to unsafe airspace conditions.

Maintenance Systems: Tampering with maintenance records could result in unsafe aircraft operations.

Statistic:

60% of aviation safety incidents involving cybersecurity are linked to human error or insider threats (ICAO, 2022).

Interconnection between Cybersecurity and Physical Security

Key Link:

Cybersecurity is a subset of aviation security, focusing on protecting digital systems from unauthorized access and malicious activities.

Examples:

Data Breaches: Unauthorized access to passenger data undermines aviation security.

Physical Security Systems: Cyberattacks on access control systems (e.g., airport gates) can compromise physical security.

Cargo Security: Tampering with cargo tracking systems can facilitate smuggling or terrorism.

Statistic:

85% of airlines have faced attempts to disrupt their systems (IATA, 2022).

Interconnection between Cybersecurity and Efficiency

Key Link:

Cybersecurity measures must balance protection with operational efficiency to avoid delays and disruptions.

Examples:

Airport Operations: Cyberattacks on baggage handling systems can cause delays and reduce efficiency.

Flight Operations: Disruption of flight planning systems can lead to inefficient routing and fuel consumption.

Passenger Processing: Cyberattacks on check-in systems can lead to long queues and operational bottlenecks.

Statistic:

The FAA NOTAM system outage in 2023 caused **11,000 flight delays**, highlighting the link between cybersecurity and efficiency.

Interconnection between Cybersecurity and Capacity

Key Link:

Cybersecurity ensures that aviation systems can handle growing air traffic demands without disruption.

Examples:

Air Traffic Management (ATM): Cyberattacks on ATM systems can reduce airspace capacity by causing delays or grounding flights.

Airport Infrastructure: Disruption of airport systems (e.g., runway lighting) can limit the number of flights an airport can handle.

Aircraft Systems: Compromised aircraft systems may require grounding, reducing fleet capacity.

Statistic:

The global aviation industry is expected to handle **10 billion passengers annually by 2040**, requiring robust cybersecurity to maintain capacity (ICAO, 2023).

Regulatory Framework and ICAO's Role

ICAO's Cybersecurity Strategy

ICAO has emphasized the need for a collaborative approach to cybersecurity across member states (ICAO Assembly Resolution A40-10, 2019).

The Global Aviation Security Plan (GASeP) includes cybersecurity as a core component.

Key ICAO Meetings on Cybersecurity

2022 ICAO Cybersecurity Symposium: Highlighted the need for harmonized standards and information sharing.

2023 ICAO High-Level Conference on Cybersecurity: Focused on integrating cybersecurity into safety management systems (SMS).

2024 ICAO Security Week: Focused on Cybersecurity of ATM systems, Robustness and Emergency response of Airport Systems, Evolution of Aviation Regulatory Landscape

SARPs and docs guiding Cybersecurity in Aviation

Chapter 18 of Annex 17 to the Chicago Convention – Aviation Security

Standard 4.9.1: Each Contracting State shall ensure that operators or entities as defined in the national civil aviation security programme or other relevant national documentation identify their **critical information and communications technology systems and data used for civil aviation purposes** and, in accordance with a risk assessment, develop and implement, as appropriate, measures to protect them from unlawful interference.

Recommended Practice 4.9.2 Recommendation: Each Contracting State should ensure that the measures implemented protect, as appropriate, the confidentiality, integrity and availability of the identified critical systems and/or data. The measures should include, inter alia, security by design, supply chain security, network separation, and the protection and/or limitation of any remote access capabilities, as appropriate and in accordance with the risk assessment carried out by its relevant national authorities.

Relevant material in ATM Security Manual (Doc 9985) - 2013

ICAO Guidance on Traffic Light Protocol for Cyber Information Sharing - 2024

Cybersecurity Policy Guidance – 2022

Cybersecurity Culture in Civil Aviation - 2022

Challenges in Cybersecurity Risk Management in Aviation

Ever evolving Threat landscape and emerging Threats

Increased Connectivity: Modern aviation systems encompass cloud computing, Operational Technology (OT), Internet of Things (IoT), mobile devices, and traditional IT infrastructure, **expanding the attack surface and leading to an increase in security incidents.**

Operational Complexity: The integration of diverse technologies has led to complex networks, making timely detection and response to security incidents challenging.

Threat vectors are increasing with rapid advancement and multi-system integration of Operational systems, Passenger Boarding systems, Biometric Systems etc.

Fragmented Systems:

Legacy systems in aviation are often not designed with cybersecurity in mind.

Lack of interoperability between safety and security systems.

Due to disparate pace of upgrades among stakeholders and interdependency of systems, cybersecurity is often prioritized lower than backward compatibility

Challenges in Cybersecurity Risk Management in Aviation – contd.

Resource Constraints:

Smaller airlines and airports may lack the budget for advanced cybersecurity measures.

Human Factors:

Insider threats like disgruntled/malicious employees, third party employees, victims of social engineering, malicious agents.

A 2023 IBM Security report found that 95% of breaches are due to human mistakes, including falling for phishing emails, using weak passwords, and mishandling sensitive data.

Past Cybersecurity incidents impacting operations

British Airways Data Breach (2018):

Compromised personal data of 500,000 customers.

Highlighted the need for better third-party vendor risk management.

Ukraine Air Traffic Control Attack (2022):

Cyberattack disrupted flight operations, emphasizing the link between cybersecurity and safety.

FAA NOTAM System Outage (2023):

Grounded flights across the U.S., underscoring the importance of system resilience

Airport and Aviation Services Sri Lanka (AASL) (2024)

Suffered a significant data breach, exposing over 7000 records, including names, national identification numbers, and passport details (Cyber Security Review,2024)

Best Practices for Holistic Risk Management

Implementation of Information Security Management System (ISMS)

Develop, implement, monitor and upgrade robust ISMS through policies – Robust Crisis Management, Business Continuity Plans, Disaster Recovery mechanisms

Integration of Safety and Security:

Develop unified risk assessment frameworks (e.g., ICAO's SMS and cybersecurity integration).

Investment in Infrastructure and Modernization:

Install, monitor, react and manage Cybersecurity infrastructure at all layers: endpoint, network (north-south, east-west), devices, servers, integration points

Establish Zero Trust Network architecture, robust Access & Authorization control and Change management practices.

Upgrade legacy systems and adopt secure-by-design principles.

Best Practices for Holistic Risk Management - contd

CyberSecurity Operations Centres (C-SOCs)

Establishing C-SOCs in the aviation sector can enhance security by providing visibility into threats, aiding investigations, and enabling proactive threat mitigation.

Collaboration and Information Sharing:

Establish and participate in platforms for sharing threat intelligence (e.g., Aviation ISAC). Follow ICAO

Cybersecurity culture, Capacity Building, Training and Awareness:

Promote Cybersecurity culture, Cyber-hygiene, 'Just culture' for self-reporting

Regular cybersecurity training for all aviation stakeholders

Emerging Trends

AI & Machine Learning in Threat Detection – Predictive analytics and anomaly detection will enhance real-time threat identification.

Zero Trust Architecture (ZTA) – Adoption of ZTA principles will minimize insider threats and unauthorized access.

Quantum Computing Threats – The rise of quantum computing may challenge current encryption methods, requiring post-quantum cryptography.

5G & Edge Computing Integration – Faster data transmission will enhance efficiency but increase cyber risks in connected aviation systems.

Recommendations

Strengthen Cyber Resilience – Implement Security Operations Centers (SOCs) and real-time threat monitoring.
Enhance Cross-Sector Collaboration – Foster cooperation between airlines, airports, ANSPs, and regulators.
Prioritize Cyber Hygiene & Training – Regular cybersecurity drills and human factor awareness programs to mitigate insider risks.
Adopt Cybersecurity by Design – Integrate security into new aviation technologies from the development phase.
Develop Post-Quantum Encryption Strategies – Future-proof communication systems against emerging cryptographic threats.
Regulatory & Compliance Evolution – ICAO, IATA, and EASA must strengthen cybersecurity regulations to ensure global standardization.

Conclusion

Aviation cybersecurity is everyone's responsibility.

Strengthening of regulations is required for global standardization of Cybersecurity practices.

A holistic approach must balance facilitation, safety, security, efficiency, and capacity.

Continuous collaboration and innovation are essential among various stakeholders.

In aviation, cybersecurity is not just about protecting systems and data; it's about safeguarding lives.

धन्यवाद | **Thank You**
नमस्ते | Namaste