CSAAP

Course One

Introduction to Cybersecurity and Airport Administration

Module One

Introduction to Airports, Airport Administration, and Cybersecurity Fundamentals

Overview of the airport environment, stakeholders, airport types, basic flight operations, and foundational cybersecurity principles relevant to airport administration.

Sponsored by the US National Science Foundation

Cuyahoga Community College

Agenda

- The Airport Ecosystem: History, Stakeholders, Types
- Connecting Airports to Cyber Risk
- Airport Governance Structures & Roles
- The Regulatory Landscape & Compliance Drivers
- Cybersecurity Fundamentals: CIA in the Airport Context
- Key Cyber Threats to Airport Administration
- Introduction to Cybersecurity Frameworks (NIST, ISO, etc.)

Objectives

- Recall data integrity/availability principles (1.1)
- Describe secure communication importance (1.2)
- Identify key federal regulations (3.1)
- Understand governance role (3.2)

A Historical Glimpse - Shaping Today's Airports

- **Early Days:** Air Mail Act (1925), Air Commerce Act (1926) → Commerce & Safety focus.
- **Growth Eras:** WPA & DLAND → Infrastructure expansion, Federal funding principles (Cost-share, Grant Assurances).
- **Regulation & Structure:** FAA Creation (1958), Part 139 Cert. (1970), Trust Fund ('Users Pay').
- **Modern Era:** Deregulation (1978 - Market forces), ATSA (2001 - TSA, Security focus), NextGen (Ongoing IT reliance).

Airport Stakeholders & Data

- **Government Entities (FAA, TSA, CBP):** Regulatory data, security info (SSI), operational directives.
  - *Need: Secure comms, data integrity.*
- **Aeronautical Users (Airlines, GA, FBOs):** PII, flight plans, operational data, financial info (leases).
  - *Need: Confidentiality, availability, integrity.*
- **Non-Aeronautical Users (Concessions, Parking):** Financial transactions (PCI-DSS), customer data, lease info.
  - *Need: Confidentiality, integrity (financial), availability (POS systems).*
- **The Community (Passengers, Neighbors):** PII (if collected), noise complaints, general inquiries.
  - *Need: Privacy, secure communication channels.*

Airport Types & Varying Cyber Needs

- **Commercial Service (Part 139 Cert.):** High passenger/data volume, complex systems (FIDS, BHS, PACS), strict TSA/FAA cyber regs likely.
- **General Aviation:** Less passenger PII, simpler systems generally, but still handle financial data, flight plans, tenant info.
  - Business/Corporate ops may have high-value data. Fewer direct cyber regs, but best practices vital.
- **Cargo Service:** High-value shipment data, logistics systems integration, supply chain vulnerabilities.
- **Joint/Shared Use:** Integration challenges between civil/military networks, differing security standards.

The Airport Environment: A Target-Rich Opportunity

- Airports blend Public Service & Business Enterprise.
- **Diverse Functions = Diverse Systems:** Finance, HR, Operations, Planning, Marketing, Security (PACS, CCTV), Building Controls (HVAC), Communications.
- **Interconnectedness:** Systems often share data (e.g., flight info feeds FIDS, gate assignments link to billing).
- **High-Value Data:** PII, Financials (PCI), Operational Plans, SSI, Contracts, Intellectual Property.
- **Reliance on IT/OT:** Critical for efficiency, safety, security, and revenue.
- **Result:** Complex environment with numerous potential entry points and high-value targets.

Airport Governance & Management

- **Sponsor Structures:** Municipality, Authority, State, etc.
- **Sponsor Role:** Sets policy, budget, risk tolerance, strategic cyber direction.
- **Executive Role:** Implements policy, manages resources, advises sponsor on cyber risks, ensures security posture.
- **Impact on Cybersecurity:** Governance dictates budget approval, policy enforcement speed, reporting lines, organizational commitment.

Regulatory Landscape & Compliance Drivers

- **FAA:** Safety-focused, with cyber implications (NAVAID integrity), Grant Assurances.
- **DHS/TSA:** Security-focused (Part 1542, SDs & Emergency Amendments, Network segmentation, IR Plans, Access Control, Patching), Part 1520 (SSI Protection).
- **Other:** EPA, State/Local data privacy laws, PCI-DSS for payment cards.
- **Compliance** → Fines, funding risks, liability.

Cybersecurity in Airports: The CIA Triad

- **Confidentiality:** Who needs access to what data? Protecting PII (employee/passenger), financials, contracts, SSI.
  - *Violation Example: Unencrypted employee records stolen.*
- **Integrity:** Ensuring data accuracy & trustworthiness. Vital for financial reports, operational schedules, security logs, stakeholder comms.
  - *Violation Example: Ransomware corrupts budget files.*
- **Availability:** Systems & data accessible when needed. Critical for payroll, billing, communication systems, access control.
  - *Violation Example: DoS attack takes down airport public website/internal network.*

Key Threats 1: Phishing & Data Breaches

- **Phishing:** Social engineering via deceptive comms.
  - *Goal: Steal Credentials, Install Malware.*
  - *Airport Admin Vectors: Emails appearing as IT, HR, FAA/TSA, vendors, executives (whaling). Fake invoices, urgent requests, fake login pages.*
  - *Impact: Compromised accounts -> Data Breach, Unauthorized Access, Malware Infection.*
- **Data Breach:** Unauthorized access/exposure/theft of sensitive data.
  - *Causes: Phishing, Malware, Insider Threat, System Vulnerabilities, Lost Devices.*
  - *Airport Admin Impact: Loss of PII (employees, possibly passengers via shared data), Financial Data (PCI violations), Contractual/Legal Info, Proprietary Plans, Reputational Damage, Fines.*

Key Threats 2: Ransomware & DoS Attacks

- **Ransomware Recap:** Malware that encrypts files; demands ransom for decryption key.
  - *Delivery: Phishing emails, exploiting vulnerabilities.*
  - *Airport Admin Impact: Critical systems locked (Finance, HR, Planning, Scheduling); Operations halted; Data loss if backups fail; Extortion costs; Reputational damage. (Availability & Integrity focus). Example: Cleveland Hopkins ransomware attack.*
- **Denial-of-Service (DoS) Recap:** Overwhelming a system to make it unavailable to legitimate users.
  - *Method: Flood servers/networks with traffic (Distributed DoS - DDoS uses many compromised computers).*
  - *Airport Admin Impact: Public website inaccessible (info dissemination fails); Internal network access disrupted for staff?; Less common target for internal admin systems vs. public-facing ones, but interconnectedness poses risks. (Availability focus).*

Cybersecurity Frameworks & Standards

- **Purpose:** Provide structure, best practices, common language for managing cyber risk.
- **Key Frameworks/Standards** in the Airport Context:
  - ***NIST Cybersecurity Framework (CSF):*** *(US, Voluntary) Focuses on Risk Management Functions: Identify, Protect, Detect, Respond, Recover. Widely adopted, flexible.*
  - ***ISO 27001:*** *(International, Certifiable) Focuses on establishing, implementing, maintaining, and improving an Information Security Management System (ISMS) based on risk assessment and controls listed in Annex A. Demonstrates mature security posture.*

Cybersecurity Frameworks & Standards (Cont'd)

- **Key Frameworks/Standards** in the Airport Context (Cont'd)
  - ***IEC 62443:*** *(International) Set of standards specifically for Industrial Automation and Control Systems (IACS) / Operational Technology (OT). Relevant for securing systems like baggage handling, building automation, airfield lighting controls. Uses concepts like Zones & Conduits.*
  - ***MITRE ATT&CK®:*** *(Knowledge Base) Catalog of real-world adversary tactics and techniques. Not a framework for management, but used within management for threat modeling, detection engineering, adversary emulation (red teaming). Helps understand how attackers operate.*

Conclusion

- **Recap:** Airports are complex ecosystems with diverse stakeholders, governance, and regulations. Cybersecurity (CIA) is vital for protecting administration (data, systems).
  - *Key threats (Phishing, Ransomware, Breaches, DoS) require structured management using frameworks (NIST CSF, ISO 27001, etc.).*
- **Key Takeaway:** Effective airport administration requires integrated cybersecurity awareness and practices.

Module 2 Preview & Questions

- Read CM Module 2 (Planning, Construction, Environmental). We will discuss securing planning data (ALPs, Master Plans), construction project cybersecurity, and protecting environmental compliance systems.
- Check LMS for readings, supplemental resources, discussion board, and quiz.
- Questions?