CSAAP

Course One

Introduction to Cybersecurity and Airport Administration

Module Four

Communications, Community Relations, Air Service & Future Trends

Overview of how airports interact with the world outside their fences and how they prepare for the future of aviation.

Sponsored by the US National Science Foundation

Cuyahoga Community College

Agenda

- Effective Stakeholder Communications & Engagement
- Airport Public Relations, Marketing & Branding Strategies
- The Air Service Development (ASD) Process
- Managing Airport Noise: Abatement Programs
- Understanding the National Airspace System (NAS) & ATC
- Future Aviation Trends: NextGen, UAVs, Commercial Space
- Cybersecurity Implications Across the Board

Objectives

- Analyze stakeholder comms vulnerabilities (1.4)
- Assess IDS in ATC (2.3)
- Apply encryption to flight ops data (2.4)
- Evaluate compliance via audits (3.3)
- Monitor/adapt practices (3.5)
- Secure tenant/contractor data (5.1, 5.3)
- Develop security for digital property management (5.4)
- Explain/evaluate vendor cyber practices (6.2, 6.4).

Stakeholder Communications & Engagement

- **Definition:** Building and maintaining relationships with all parties interested in or affected by the airport.
- **Key Stakeholders:** Airport Board/Sponsor, airlines, tenants, employees, passengers, community groups, government agencies, media.
- **Airport Board/Sponsor Relations:** Critical for governance, policy, funding. Requires secure, confidential communication.
- **Broader Engagement Tools:** Websites, social media, newsletters, public meetings, advisory committees (e.g., for noise).

Stakeholder Comms. & Engagement (Cont'd)

- Cybersecurity Concerns:
  - *Securing communication channels for sensitive board materials (e.g., encrypted emails, secure board portals).*
  - *Protecting stakeholder databases (PII, contact details, preferences) from breaches.*
  - *Ensuring authenticity of official airport communications (preventing website spoofing, social media account takeover).*

Airport Public Relations & Media (Cont'd)

- **PR Goal:** Proactively shape public perception, manage the airport's image, and serve as the primary source of information.
- **Media Relations:** Building relationships with journalists, issuing press releases, responding to inquiries, arranging interviews.
- **Crisis Communications Plan:** Essential component. Defines roles, procedures, messaging during incidents. Designated spokesperson.
- **Social Media in PR:** Rapid information dissemination, direct engagement, but also risk of misinformation.

Airport Public Relations & Media (Cont'd)

- Cybersecurity Concerns:
  - *Securing official social media accounts (MFA, strong password policies, limited admin access).*
  - *Monitoring for and actively combating disinformation or impersonation campaigns.*
  - *Protecting digital copies of the Crisis Communications Plan from unauthorized access.*
  - *Ensuring website integrity to prevent defacement or hosting of malicious content.*

Airport Marketing & Branding

- **Purpose:** Promote airport services, attract passengers and businesses (including non-aeronautical revenue), build brand loyalty.
- **Marketing Mix (The 4 Ps):** Product (flights, facilities, services), Price (value proposition), Place (accessibility, convenience), Promotion (advertising, PR).
- **Branding:** Creating a unique and positive identity for the airport (logo, tagline, experience).
- **Digital Marketing Tools:** Websites, mobile apps, social media, email marketing, Customer Relationship Management (CRM) systems, loyalty programs.

Airport Marketing & Branding (Cont'd)

- Cybersecurity Concerns:
  - Protecting customer PII collected through marketing channels (GDPR, CCPA compliance).
  - Securing CRM systems and marketing automation platforms from data breaches.
  - Preventing unauthorized access or defacement of digital marketing assets (websites, apps).
  - Ensuring security of online payment systems if marketing links to direct sales (e.g., parking).

Air Service Development (ASD)

- **Goal:** Attract, retain, and expand air service to benefit the airport and community.
- **Key Process Steps:** Market analysis (catchment area, leakage), airline targeting, business case development, route forecasting, incentive negotiation, ongoing relationship management.
- **Data-Intensive:** Relies on passenger demand data, economic data, airline operational/financial data (often confidential), route profitability models.
- **ASD Incentives:** Fee waivers, marketing co-ops, revenue guarantees (require careful FAA review).

Air Service Development (ASD) (Cont'd)

- Cybersecurity Concerns:
  - *Protecting highly sensitive and proprietary ASD analytical data.*
  - *Securing data shared by airlines under NDAs.*
  - *Ensuring integrity of financial models and forecasts used in business cases.*
  - *Vendor risk management for ASD consultants handling sensitive data.*

Airport Noise Abatement (Part 150/161)

- **Context:** Balancing airport's economic role with community quality of life.
- **FAA Part 150:** Airport Noise Compatibility Planning. Voluntary program.
- **Noise Exposure Maps (NEMs):** Depict DNL contours.
- **Noise Compatibility Program (NCP):** Airport's plan for mitigation.
- **FAA Part 161:** Airport Noise and Access Restrictions. For proposed operational restrictions.
- **Mitigation:** Land acquisition, sound insulation, preferential runways, modified flight tracks.

Airport Noise Abatement (Part 150/161) (Cont'd)

- Cybersecurity Concerns:
  - *Integrity of data from noise monitoring systems (often networked OT devices).*
  - *Secure storage and controlled access for NEMs, NCPs, and related sensitive community data (e.g., addresses for sound insulation programs).*
  - *Protecting flight track analysis systems used for noise modeling.*

National Airspace System (NAS) & ATC

- **NAS Definition:** Comprehensive U.S. network of airspace, people, procedures, facilities, and equipment for safe and efficient flight.
- **Airspace Classes:** A, B, C, D, E, G – define rules and services.
- **Air Traffic Control (ATC):** Managed by FAA.
- **ATCT (Airport Traffic Control Tower):** Airport surface & vicinity.
- **TRACON (Terminal Radar Approach Control):** Airspace around busy airports.
- **ARTCC (Air Route Traffic Control Center):** En route airspace.

National Airspace System (NAS) & ATC (Cont'd)

- Cybersecurity Concerns:
  - *Concerns revolve around the interface that the airport has with these systems and programs*
  - *Understanding critical reliance on ATC.*
  - *Secure any airport systems that interface with ATC data (e.g., flight information).*

NAVAIDS & Airport Capacity Challenges

- **NAVAIDS (Navigational Aids):** Provide guidance. Ground-based (VOR, ILS) & Satellite-based (GPS/WAAS).
- **Airport Capacity:** Max aircraft operations in a period. Influenced by runway/taxiway layout, gates, weather, ATC.
- **Delay:** Occurs when demand > capacity. Can propagate through NAS.
- Cybersecurity Concerns:
  - *Like NAS/ATC concerns, this revolves around the airport interface*
  - *Ensuring integrity of data from any airport-owned/maintained NAVAIDS (e.g., AWOS, PAPI).*
  - *Physical security of all NAVAIDS on airport property.*
  - *Secure maintenance access for any NAVAID components supported by airport staff.*

Future Trends – NextGen

- **NextGen:** FAA's comprehensive modernization of the NAS.
- **Goals:** Enhance safety, increase efficiency & capacity, reduce environmental impact.
- Key Technologies:
  - ***ADS-B (Automatic Dependent Surveillance-Broadcast)*** *– GPS-based surveillance.*
  - ***SWIM (System Wide Information Management)*** *– Digital data sharing.*
  - ***DataComm (Controller-Pilot Data Link Communications)*** *– Digital text comms.*
  - ***PBN (Performance Based Navigation)*** *– Precise, satellite-based routes.*
- Cybersecurity Concerns:
  - *Increased connectivity & data reliance introduces new vulnerabilities.*

NextGen Cybersecurity Challenges

- **ADS-B Security:** Broadcasts are unencrypted; vulnerable to spoofing (false targets) and jamming. Requires mitigating systems and procedures.
- **SWIM Security:** Protecting integrity, availability, and confidentiality of vast amounts of shared data from diverse sources. Authentication & authorization are key.
- **DataComm Security:** Ensuring authenticity and integrity of digital controller-pilot communications; preventing unauthorized messages or manipulation.
- **PBN Security:** Integrity of navigation databases (aircraft & ground) is critical for safe execution of precise routes.
- Airport systems will increasingly interface with NextGen, inheriting some risks and responsibilities for securing local interfaces/data.

Future Trends – UAVs & Commercial Space

- **UAVs (Drones):** Rapid proliferation. Significant safety/security concerns for airports (unauthorized incursions).
- **C-UAS (Counter-UAS) Systems:** Detect, track, identify, mitigate unauthorized drones.
- **Commercial Space Transportation:** Growing industry; licensed spaceports (some co-located at airports). Unique airspace management & safety needs.
- Cybersecurity Focus:
  - *UAVs: Securing C-UAS systems (data integrity, preventing spoofing/jamming of C-UAS), addressing malicious drone payloads/activities.*
  - *Spaceports: Protecting sensitive launch/trajectory data, securing specialized IT/OT for ground control, telemetry, and range safety.*

Conclusion

- **Recap:** Airports manage complex external communications, PR/marketing, ASD, noise, and interact with a dynamic NAS (NextGen, UAVs, Space).
- Cybersecurity underpins the trust, data integrity, and system availability required for all these functions.
- This concludes our CM-focused content.

Module 5 Preview & Questions

- We will shift to broader IT & Cybersecurity Management Strategies for airports, drawing on external resources while referencing CM context
- Check LMS for readings, supplemental resources, discussion board, and quiz.
- Questions?