Building a Cybersecurity Team
The Airport Perspective

Background

- Department of the Interior
  - CIO for Indian Affairs
  - CIO for the National Park Service
- Los Angeles World Airports
- Aviation-ISAC

Background

- Past Chair of ACI World Cybersecurity Taskforce
- Past Chair of ACI-NA Cybersecurity Sub-committee
- ACI Cybersecurity Trainer
- Author/Editor of most ACI Cybersecurity Handbooks
- Co-Author Safe Skies Guidebook on Cybersecurity
- (ISC)2 Past Advisory Board Member
- CISSP Trainer

Challenges in Hiring in the Federal Government 1998-2006

- Always seemed to be in an agency or government-wide hiring freeze
- Often had to rely on transfers/reassignments so as not to increase head count
- Lower graded positions didn't have enough experience, and when establishing a new organization didn't have time to do much training
- Couldn't match private sector salaries for higher graded positions with true cybersecurity experience
- At that time, CISO was not a recognized position title (could make it a working title)
- Typically had to hire non-cybersecurity personnel and train OTJ
- Could not require CISSP or other certifications

Challenges in Hiring Los Angeles World Airports 2007-2016

- City of LA Civil Service system similar to the federal system of the 1960s and before
- Required a CS entrance exam
- Had to be placed on a general civil service list
- The list was open to all city departments
- Could only select from the top three
- It gets worse from this point on …

Aviation-ISAC Present

- No procedural requirements
- Decent pay – but not equivalent to private sector aviation companies
- Mediocre Benefits – couldn’t attract current airport personnel
- Sought someone with airport experience, then aviation – couldn’t find many candidates with such experience

Airport Cybersecurity

Airport Characteristics

- Airports Differ Greatly in Traffic Counts
  - Small
  - Medium
  - Large
  - Category X (DHS Designation)
  - General Aviation Airports
- Financial Resources
- Physical Size

Airports as a Local Community Member

- Economic Driver
- Projects the Image of the Local Community
- Critical Transportation Node
  - In many locations, the focal point for multi-modal transportation
- Critical Infrastructure in an Emergency
- Oversight by Local, County, or State government
- Draws Constant Media Attention
- Cybersecurity Attacks are a major embarrassment

Airports as a Business Entity Impacts Cybersecurity

- Non-Profit Organizations
- Regulated by the FAA
  - AIP Grant Funding Serves to Limit Airport Discretion
- Passenger Facility Charges (PFCs) – added to airfares
- Non-airline Revenue (Concessions, Parking, other Outside Businesses)
- Three Airline/Airport Financial Arrangements
  - Compensatory
  - Residual
  - Hybrid
- Governing Bond Legislation

Airports as an Airline Business Partner

- Airlines Seek a Financially Viable Location to Operate
- Airport Use and Lease Agreement
  - Rates and Charges Methodology
  - Airline Oversight of Capital Improvements

- Growing Trend to Common Use Passenger Processing (CUPPS)
  - Maximizes Gate Usage
- Managed Services
- Shared IT Infrastructure
- Airports with cybersecurity responsibility to airlines

Airports Serving Airlines

- Gate Management
- Fuel Services (Consortiums)
- Airline Co-Ops for Terminal Management
- Managed Technology Services
- Terminal Maintenance
- Terminal Concessions
- Credentialing
- Security Checkpoints
- Stress-free and Relaxed Passengers
- New Technology for Passenger Processing
- All new technologies further stress airport cybersecurity capabilities

Airport Technology

- IT Departments Vary Greatly in:
  - Titles
  - Number of Staff
  - Responsibility
  - Oversight
  - Budget
  - Cybersecurity Awareness and Responsibility
- Systems
  - Common Use
  - Incident Management Systems
- May Share IT Resources with Local Government
- External Oversight (Cities, Port Authorities)

Airports and Airlines Working Together

- Technology
- Common Use
- Sharing Resources
- Wi-Fi
- Terminal VoIP
- Multi-Use Flight Info Display Screens
- Cybersecurity
  - Certification and Accreditation
  - PCI/DSS Compliance
- Physical Security Systems
- Communication and Collaboration

Airports as a Target

- Critical Component in the *Aviation Supply Chain*
- Airports Could be a threat vector to airline operations
- Airports have fewer resources than airlines and aircraft manufacturers
- Airports, like airlines, are a target for physical and cyber attacks
- Airport Industrial Control Systems could become a major target in the future

The State of Airport Cybersecurity Today

- Needs significant improvement system-wide
- Only larger airports typically have appropriate cybersecurity staff
- Medium and smaller airports may have no dedicated cybersecurity team
- Cybersecurity is not typically an issue that gets airport management attention … until it is too late
- For many years, airports have not experienced many attacks
- That changed in 2018 when ransomware and credential theft attacks started hitting airports on a frequent basis

The State of Airport Cybersecurity Today

- No common framework specifically for airports
- No federal measurement for cybersecurity compliance
- No requirement to staff cybersecurity positions
- Reliance of manufacturers to ensure hardware/software has no vulnerabilities
- Reliance on outside consultants
- Few airports have a full risk management program and strategy
- Few airports have a cybersecurity disaster recovery and business continuity plan
- Few airports have a cybersecurity IT governance structure

Why is Airport Cybersecurity Lacking?

- Airports are non-profit entities, only in existence to serve airlines
- It is the airport's objective to keep costs as low as possible for the traveling public
- There are many competing demands for airport revenues and cybersecurity does not rank high
- It is difficult to get adequate resources for cybersecurity hiring
- There is no federal mandate for specific cybersecurity practices
- Airports do not take advantage of cybersecurity intel opportunities
- Many airport IT directors, CIOs not focused on cybersecurity

Airport Cybersecurity Hiring Challenges

- Finding experienced cybersecurity personnel
  - Few with aviation experience
- Retaining cybersecurity personnel
- Finding cybersecurity personnel with appropriate credentials
- Salary and Training Opportunities
- No collaboration through meetings and conferences minimal due to low travel resources
- Airports have a variety of hiring processes some easy, some difficult

Value of Certifications

- (ISC)2 Certified Information Systems Security Professional (CISSP)
  - Held by **56 percent** of cybersecurity professionals
- CompTIA Security+
  - Held by **19 percent** of cybersecurity professionals
- Certified Information Security Manager (CISM)
  - Held by **17 percent** of cybersecurity professionals
- Certified Information Security Auditor (CISA)
  - Held by **16 percent** of cybersecurity professionals

Darril Gibson in *Security+*

Questions

Comments

Discussion

Thank You