Data Security and Privacy at Commercial Airports

GateKeeper Systems

Data Security and Privacy at Commercial Airports

As much as it may be wished otherwise, airports are not exempt from the perils of cyber-attacks on their computer systems. For a variety of purposes, ranging from thrill-seekers to criminals out to get all types of information for financial gain, unwanted attention is continually focused on airport IT systems. Protecting these information and technology assets is growing more complicated and more important each day.

Data Collection: An Overview

Airports and their tenants collect vast amounts of data daily. Airline schedules, concessions sales, payment information (credit cards), passenger information, law enforcement activity, immigration data, etc. are all being generated in various technology-based systems. Another significant example of the data being collected is from your ground transportation system, the table below lists the major, but not all, modes used along with the general types of information collected. Data is generated, maintained, and analyzed on driver, vehicle, and company activity. This data also frequently includes the credit card information on thousands of passengers. At most airports, this stream of information is growing at a rapid rate.

Ground Transportation Modes/Data Collection

Ground Transportation Mode	Personal Information	Vehicle Information
Public Parking	X	
Taxicab	X	X
TNC- App-Ride	X	X
Courtesy		X
Charter Bus		X
Public Trans- Bus		X
Limo	X	X
Airport Shuttles		
Auto Rental/Parking Shuttles		X
Shared Ride	X	X

Not only is the amount of data growing, but the advances in technology are allowing new and more sophisticated uses of that data, which includes analysis by aggregating the data into a few large “Business Intelligence” (BI) systems that are focused on finding ways to improve the customer experience at airports. The data is also being used to automate many of the labor-intensive functions that create lines and waste time (automated baggage check-in, for example), provide services that have not been available in the past (such as ordering, delivering, and paying for a meal while waiting in a gate lobby), monitor wait times, and other new product ideas that are introduced almost daily. This data is extremely useful to airports and airport tenants in monitoring the results of management actions and helps identify new ways to improve the passenger experience.

Privacy & Security:
Data Collection's Twin Problems

The value of this rapidly evolving technology environment requires airport management attention in at least two key areas that are related, but different:

1. Data Privacy - Intense public concern is being directed at data related to individuals as well as confidential organizational data. Knowing what data is being collected, who is collecting the data, how is it being used, who has access, and what are an individual's right to decline to have their personal information collected are all important for your airport to understand.

2. Data Security - In addition to finding ways to obtain, organize, and analyze these vast streams of data, airport management must address "cyber security" concerns about the potential for data breaches of airport systems that can result in the unauthorized access to information stored in airport or third-party vendor systems.

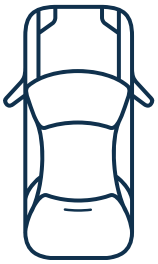
Know Where the Data is Coming From

It is not news that airports collect and maintain a significant amount of information on the people and vehicles that provide ground transportation services. The table below illustrates the type of data that is currently being collected by airports.

PERSONAL INFORMATION

- NAME
- ADDRESS
- E-MAIL ADDRESS
- CREDIT CARD INFORMATION
- PERMIT INFORMATION
- VIOLATION INFORMATION
- SS#
- DRIVER'S LICENSE #

VEHICLE INFORMATION



- TRIP ACTIVITY
- MAKE
- COLOR
- MODEL
- LICENSE PLATE #
- VIN
- VEHICLE LOCATION
- FEES CHARGED
- INSPECTION INFORMATION

The definition of data that is "personal" is still evolving and the data being gathered from a variety of systems almost certainly contains or will contain "private/personal" data on employees, tenants, and/or the general public. This data can be assembled to create a very complete picture of individuals and their visits to the airport.

Enact Privacy Safeguards

To address this "privacy issue", privacy requirements are being enacted that impact airport programs. Some of the key areas that all airports need to incorporate into privacy policy and procedures include:

1. Non-Disclosure Agreements ("NDA"): While having an NDA in place will not thwart a cybercrime, it will provide a confidentiality agreement with third parties and will help define actions if the information is disclosed.
2. General Data Protection Regulation ("GDPR"): The European Union's (EU) General Data Privacy Regulation went into effect on May 25, 2018, and contains important operational requirements concerning data minimization, accuracy, accountability, purpose and storage limitations, and data protection that will require impacted organizations to make technology and administrative changes. The GDPR also mandates that companies demonstrate compliance, which requires the existence of policies, procedures, and documentation mechanisms.
3. California Consumer Privacy Act ("CCPA"): The California Consumer Privacy Act (CCPA) went into effect on January 1, 2020, codifying enhanced privacy rights and consumer protection for California residents. Consumer data privacy rights will be extended to allow residents to request, from businesses, the categories and specific elements of personal information (PI) that the business collects about the consumer, the categories of sources from which that information is collected, the business purposes for collecting or selling the information, and the categories of third parties with which the information is shared.
4. New York Privacy Act: This policy is currently in the New York Senate's Consumer Protection Committee. If passed, it will give New York residents sweeping, comprehensive, and empowering consumer privacy rights.
5. State privacy laws: Each state has some level of privacy requirements or breach/loss of data notification guidelines, so understanding the requirements by state is highly recommended for legal and compliance purposes.

Data Security Safeguards

In addition to the "data privacy" issues presented by the gathering and storage of data in airport or airport-related systems, a significant risk exists for an accidental or intentional breach of the security of one or more of the systems which contain all types of data (private, confidential, personal, or operational) to parties not authorized to have or use that data.

Airport IT systems are growing in complexity, and a significant number of airports are part of a city, county, or other organization that has implemented programmatic "links" to enterprise level systems that are a very attractive target for cyber criminals.

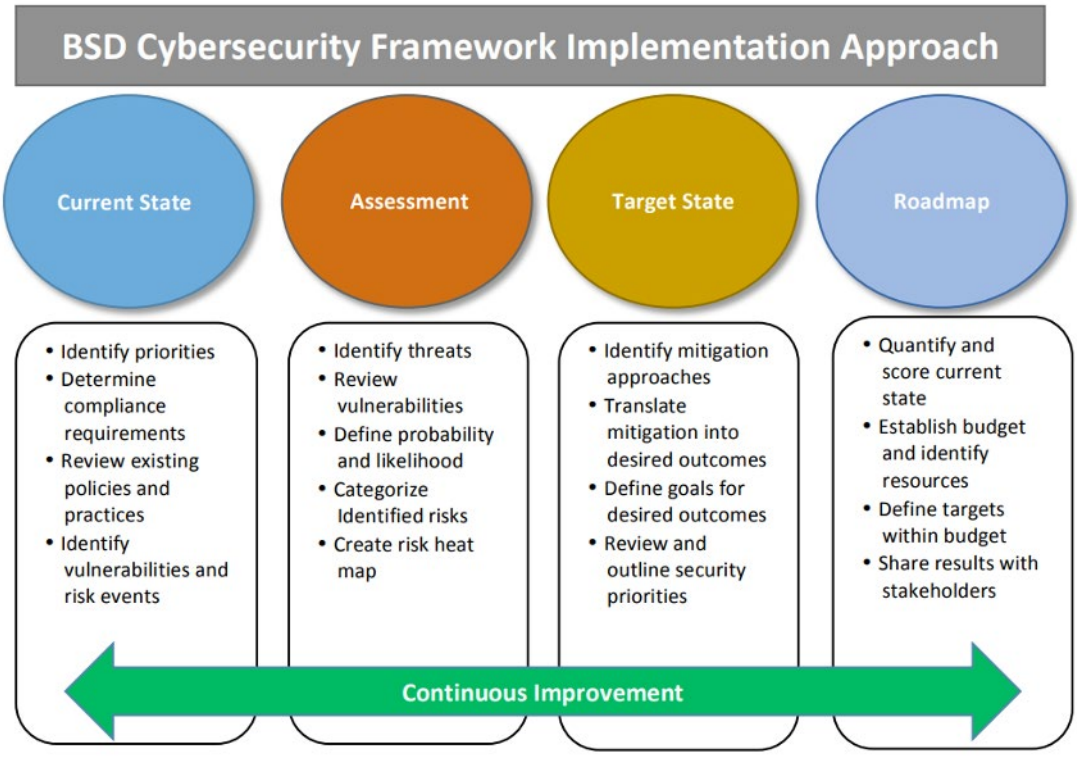
It is also necessary for airports to address the risk of employees with access to systems to be the source of a breach. This risk includes accidental acts that transmit or publish airport data to unintended recipients as well as intentional acts performed by personnel who intend to harm the organization.

As data privacy and security issues become more and more important, the need for airports to implement security measures is paramount. Let's examine some of the ways the security of airport data can be enforced.

Plan Ahead

The media will continue to issue stories on new data security breaches at companies large and small, federal, state and local governments, and even airports. There is no reason to expect the risk of a data security breach will lessen or go away, so airports need to find a way to minimize the chance of a breach and also to develop a plan to handle an actual breach. Implementing a program that will stop all cyber-attacks is not technically possible and would be cost prohibitive to implement, even if it were available. Therefore, being prepared for a possible breach is essential.

A large number of models have been developed to guide organizations such as airports in developing a comprehensive approach for their cyber security programs, one example that illustrates the areas of emphasis that should be included is shown below.



Internal Efforts

Right now, there are steps every airport can take to help secure their data. These steps include:

1. Identify where confidential data and Personally Identifiable Information ("PII") resides within the airport's environment. It is critical to identify the types of information, specifically related to customer PII data, and identify where that information is housed, what systems interact with it, and where can it go. A data flow diagram is a helpful tool to identify these items. Once that is established, additional measures can be put into place.

2. Risk Assessment:
    - Develop an inventory of data and systems used by the airport that have personal, confidential, proprietary and/or operational data as well as a list of the data being generated and stored.
    - Identify the purpose, use, and authorized users of the data and systems.
    - Identify the risks of privacy and security threats for personal information.
    - Perform SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis for systems and data considered in-scope to determine areas of weakness and determine if those weaknesses should be included as an identified risk.
3. Communicate with employees and vendors the importance of the proper use and protection of airport systems (and data), as well as the policies and procedures that are in place to minimize the threats and risks.
4. Conduct a review of vendors and corresponding access to data and systems (i.e. parking, GTMS, GT Operators, taxi, limo, shuttles, TNC) and evaluate the adequacy of their privacy and security programs.
5. Adopt and publish a privacy policy that addresses the airport's handling of personal data.
6. Develop and implement a "Privacy & Security" policy for employees.

External Efforts/Resources

Beyond the internal steps which can be taken, there are several resources from outside the existing airport/ internal IT infrastructure which can help secure data:

1. Obtain consultant assistance when resources or experience are required.
2. Request vendor/third-party security certifications such as ISO 27001, NIST CSF, HITRUST, and FedRAMP.
3. Consider completing System and Organization Controls Assessment ("SOC") assessments through a third-party independent auditor to assess the design and implementation of security controls.
4. Gain an understanding of state, national and international legislation related to personal information or data that should be protected or accessed by those with assigned roles and responsibilities.
5. Consider performing Payment Card Industry (PCI) assessment activities based on the volume of card transactions or the need for securing card related data.

Summary

Data Privacy and Security are issues that are here to stay for airport managers. The potential for serious consequences of a data breach provides more than enough motivation to create a properly designed and implemented plan, which identifies policies and procedures to mitigate the chance of a breach and a specific action plan to address an actual breach.