The Challenges of Protecting US Airports

by **David Geer**

Inside this report ...

Executive Summary
Risks
Vessel Identifcation Technologies for Water Side Perimeter Security
Recommendations
The Morpho Thumb for Reading Thumb Prints
Action Plan for CSOs
Resource File

Executive Summary

[return to top of report]

US airports have come under strict security guidelines from the Transportation Security Administration (TSA), which took on what were formerly the Federal Aviation Administration's (FAA's) civil aviation security duties. The TSA, which is currently part of the Department of Transportation, is expected to come under the Department of Homeland Security in the coming months.

The TSA has issued Transportation Security Regulation 1500 (commonly referred to as TSR 1500), which is the 49 Code of Federal Regulations (CFR) chapter 12, parts 1500 through 1550. TSR 1500 is a document, a set of guidelines, and a legal mandate stipulating the results that airport security must produce.

In nine parts divided into varied chapters, parts, subchapters and subparts, TSR 1500 defines all the goals that security measures at every airport must achieve. These include, but are not limited to, the securing of airport property and screening areas, as well as employee screening itself. For example, TSR 1500 details the markers that can void an application for security clearance at an airport, including some 30 different types of felony convictions.

TSR 1500 is results-oriented rather than means-oriented. Because each of the 429 airports regulated under TSA is so unique, no one set of methods could possibly arrive at the necessary levels of security required of all airports. Each airport defines a uniquely different path toward meeting TSR 1500 stipulations.

The best and tightest security measures available could be combined to achieve more than sufficient levels of airport safety in the US, but airports cannot afford to pay the high cost that would entail. Barring government assistance, this climate is likely to persist.

Risks

[return to top of report]

Airports in the U.S. have come upon the same heightened security risks of other nations beset with terrorist threats. These threats bring to light a cumbersome list of airport security risks that must be addressed.

1. Lack of government funding

If the mandated results of airport security (which are also necessary and desirable and astronomic in cost) are not funded at least in part by the federal government, airports, which are currently wedged between rising expenses and falling traffic and income, will not be able to afford sufficient security measures. This will lead to non-compliance.

2. Insufficient perimeter protection

Airports have huge and mostly highly accessible perimeters. Some have water side perimeters (near waterways of various breadth and type, some of which permit entrance by boat). Some rely only on fencing to prevent entry. There is little or no electronic surveillance of airport perimeters, making access to the Air Operations Area as easy as a pair of wire cutters. What is often miles of perimeter makes it possible to drop weapons over fencing for later retrieval by an inside operative.

Figure 1. Vessel Identifcation Technologies for Water Side Perimeter Security

[return to top of report]

3. Inadequate control over access to the AOA

The Airport Operations Area (AOA) is frequently accessed by catering, maintenance, and oil and gas people who are working and moving around near the airplanes. These individuals are not adequately badged and background checked.

4. Identity theft

Identity theft becomes an issue of airport security as it enables the circumventing of measures like access control. An identity thief could acquire false credentials and usurp allowed access through an illegal ID.

5. Wireless infrastructure

Popular for its mobility, flexibility and quick roll out, wireless infrastructure is likely to increase in adoption at airports for use by mobile employees like baggage handlers and security guards. With wireless infrastructure comes security issues tied to its fundamentally insecure nature. In addition, if users who move from assignment to assignment and airport to airport aren't adequately managed and their access isn't changed accordingly, there is a risk of unauthorized access. If wireless networks are not segmented from wired networks, there is the risk of passing insecure data over other airport infrastructure.

6. Confusion over division of security responsibilities

Between the TSA, local police and airport security all responding to incidents, the distribution of responsibilities for answering alarms, dispatching officers and apprehending suspects must be well coordinated.

7. Near proximity, non-secured, public access

In the current environment, someone could drive a van full of fertilizer and diesel fuel onto airport property, and into the public parking area in front of the airport unchecked. This would cost lives and shut the airport down, creating a massive economic impact on the airport's business and on the U.S. economy. There would also be psychological damage.

8. Software risks

- All airplanes are now essentially "run" by software that interfaces with pilots through buttons and other controls.
- Air traffic control is run by software.
- Throughout the airport, web-based applications are used for ease of distribution. Rather than deploy an application to every computer, a single web server is installed from which individuals can retrieve applications to their workstations.

Software can fail, crash, exhibit bugs, have weak code or be infiltrated or infected with viruses. Thus, modern aviation is subject to all the risks inherent to software-based enterprises.

9. Identity management

Positively identifying airplanes, computers and people during the hand off of an airplane from one city to the next for example, and during every other process of air traffic control, is essential. There are many system users and means of entry to monitor.

10. Lack of data fusion and integration

It is vital to be able to see and control the big picture in airport security around the clock. This requires a complete integration of IT, physical security and video surveillance data through integrated security systems and products.

There needs to be continuity in tracking persons, baggage and other tangibles from the time they enter the airport until they leave via plane or other means.

11. Lack of communication

There is a lack of communication between parties from the airport staff to the airport tenants to the governmental agencies, and within each group as well.

Standards (uniform standards) for data transmissions between groups is necessary so that airport systems, TSA and FAA systems and other local systems can communicate.

Recommendations

[return to top of report]

These recommendations directly and indirectly address key risks and issues in airport security.

1. Protect the perimeter.

Current perimeter security measures need to be assessed. An evolution of perimeter security, through a layered physical and technical approach, applying state-of-the-art products and services, needs to begin.

2. Screen and badge all support company employees.

Airport support services need to better screen the people they hire. A single, uniform, standard Badging/ID system needs to be adopted that applies to all non-passengers and non-consumers on the airport property.

3. Layer both IT and physical security.

Layering of IT security includes the several measures of any business IT department including network and application layer encryption, VPNs, tunneling, security policies and access controls, firewalls, intrusion detection, and constant real-time network monitoring.

Layering of physical airport security means using several measures in tandem. These can include Closed Circuit TV (CCTV), biometrics, badging, hardened glass and frames at doors and windows, and new and advanced physical security technologies.

Figure 2. The Morpho Thumb for Reading Thumb Prints

[return to top of report]

4. Set up incident response and emergency response policies.

Maintain a detailed incident response policy and procedures that cover everyone's duties, interaction and chain of command to mitigate incident handling.

Emergency response policies and procedures provide security in the event someone gains illegal access. An incident and emergency response planner may need to be contracted.

5. Use state-of-the-art technologies.

Keep up on proven technologies in other airports from around the world. Use, customize and improve on these techniques.

Examples of new technologies include:

- Modern CCTV, which now uses digital video recorders instead of tape. Video surveillance data can be retrieved and compared instantly. The storage media is much smaller with much greater capacity.

- Video surveillance can also be automated.

- With the use of a proprietary tool from Object Video, specific objects can be detected in video, providing the opportunity to detect significance in video without viewing all the footage.

- Perimeters can be secured efficiently and cost effectively. A product called Fiber Sensys from CompuDyne deploys fiber optic sensing cable in any environment (heat, cold, inside most any material) to detect access or disturbance. It can travel lengthy perimeters in fence, in the ground, in walls and still pick up movement. It is uniquely suited to airports due to its lack of electrical emanations; it won't interfere with airport communications or other electronics.

When someone crosses that barrier, thermal imaging cameras or other CCTV cameras can be set to zoom in on the point of disturbance. The heavy fiber optic cable can be laid out over long distances without an electrical boost. There is no need of electrical connections out to the perimeter. It can be laid in brick or cement and someone scaling the wall will call an alert. Future versions of the product will pinpoint much more exactly the specific location of the disturbance, rather than within a certain length of cable as with the current version. Product developments will also shortly enable the ability to define what type of event occurred at the point of movement.

6. Integrate for a seamless picture of airport security.

Seamlessly integrate physical security hardware in order to pull together a global picture of airport security for security personnel. Coordinate efforts from a command center where all information can be retrieved and assessed as one element.. Being able to coordinate between and among airports in a nationwide situation is also crucial.

7. Address software risks.

Secure code before and during use in critical applications such as the flying and landing of planes, or communicating, or handing off flights from locale to locale. Use modern software tools to determine how safe and secure the code is. Test every entry point for possible hacks.

One of the latest hacking procedures is to enter unexpected input. This kind of hack can be used in most any program, especially websites, web applications and databases. The broader the complexity of the software, the harder it is to tell where a weakness may lay.

Good security practice dictates checking every possible combination and permutation of input, looking for security holes.

8. Partner wisely.

Partnering with those companies that are dedicated to or have a vested interest in the airport industry will help insure top quality security efforts cost effectively.

Table 1. Action Plan for CSOs

[return to top of report]

Action	Purpose
Protect the perimeter.	To prevent the illegal entry of persons or devices onto airport property.
Screen and badge all support company employees.	To ensure all airport workers are known and trusted.
Layer both IT and physical security..	To provide multiple levels of security for extra protection.
Set up incident response and emergency response policies.	To respond immediately to security violations.
Use state-of-the-art technologies.	To afford the best chance of detecting and preventing airport threats.
Integrate for a seamless picture of airport security.	To ensure all security systems and personnel are working in concert.
Address software risks.	To prevent hackers and other miscreants from penetrating key systems and applications.
Partner wisely.	To ensure airport business partners are competent, safe and reliable.

Resource File

[return to top of report]

CompuDyne: http://www.compudyne.com/
Johnson Controls: http://www.johnsoncontrols.com/
Language Analysis Systems: http://www.las-inc.com/
Object Video: http://www.objectvideo.com/
TSA: http://www.tsa.dot.gov/

About the Author

[return to top of report]

David Geer specializes in technical and business journalism. He has authored more than 100 technology and business articles for a range of publications. Mr. Geer can be contacted via email: d@geercom.com.
