5-1-2014

The Breach of Security at San Jose's Airport Raises Broader Issues

Brian M. Jenkins
NTSCOE

The Breach of Security at San Jose's Airport Raises Broader Issues

by Brian Michael Jenkins
Director, Mineta Transportation Institute's National Transportation Safety and Security Center and Special Advisor to the President of RAND Corporation

This Transportation Security Perspective is the fifth in a continuing series produced by the National Transportation Safety and Security Center of the Mineta Transportation Institute. These examine major terrorist attacks and trends in terrorists targeting surface transportation. Previous perspectives include the bus attack in Abuja, Nigeria, the terrorist bombings in Volgograd, Russia; the assault on passengers at the Kunming train station in China; and more.

The recent breach of security at Mineta San Jose Airport, in which a teenager sneaked on to the airfield and hid in the wheel well of a Maui-bound flight, raises a number of broader security questions. Security clearly failed. How someone was able to climb the airport's perimeter fence, approach the passenger terminal, hide for more than six hours, then gain access to an airplane about to take off, will be the subject of a thorough review.

It is not yet known what that investigation will tell us. Although an airport surveillance camera reportedly picked up an unidentified intruder on the tarmac, it appears that security personnel at the San Jose airport were unaware of the breach before the stowaway alighted from the plane in Hawaii. A Congressional hearing pointed out that only weeks before the incident, the Department of Homeland Security's Transportation Security Administration (TSA) had reviewed and approved the airport's perimeter security measures. So was this a failure of performance by the airport? Or are the existing standards inadequate, requiring stronger security?

Most people think of airport security only as it applies to passengers boarding aircraft. However, those charged with security must think in terms of 360-degree security—not only screening passengers coming through the terminal, but also preventing unauthorized access to the aircraft from the air operations side of airport. That requires preventing outsiders from breaching the airport perimeter while ensuring the reliability of insiders who have legitimate access to the airplanes and airside facilities.

Perimeter breaches are not unusual

Although perimeter security has increased, breaches of that security at U.S. airports are not uncommon:

- In January 2010, police arrested an intoxicated man with a knife who had climbed over the security fence at the Los Angeles International Airport. A month later, police arrested two more airport fence climbers. Another determined but disturbed individual repeatedly climbed the fence at LAX and was taken into custody several times.

- In 2010, another teenage stowaway slipped into the airport at Charlotte, North Carolina and hid in the wheel well of a Boston-bound airplane. He fell to his death as the plane approached its destination and dropped the landing gear.

- In 2012, a stranded jet skier swam to shore, climbed an 8-foot fence, and walked across two runways past security cameras and motion detectors at JFK International Airport in New York.

- In 2012, a drunk driver crashed his SUV through a gate and drove onto the runway at Philadelphia's airport.

- On Christmas Day 2013, an inebriated man climbed a fence at Sky Harbor International Airport in Phoenix and ran across the tarmac.

- The same day, a man dressed as a woman climbed over a security fence at Newark Liberty International Airport in Newark, New Jersey. Although captured on video, his presence went undetected for a day.

The violators in these recent incidents could be described as desperate, drunk, or disturbed. None were terrorists. Their actions were unplanned or improvised, which seems to give the disorganized adventurer an advantage over more calculating adversaries. Deterrence—the prospect of failure or arrest—has no effect on them. Oblivious to security, they do unexpectedly stupid things. In most cases, courts treated their crimes as misdemeanors.

Asylum seekers seem to account for most of the cases abroad in which they stow away in the wheel wells. Most of them die from lack of oxygen or hypothermia, or they are crushed when the landing gear comes up, or they fall to their deaths when it is lowered. In 2013, however, a team of eight well-informed and heavily armed robbers, dressed as police, cut through the perimeter fence at Brussels Airport. They drove up to a passenger plane in two vehicles just as diamonds were being loaded, held the crew and guards at gunpoint, and made off with $50 million in precious stones.

Hijackings, bombings are the real fear

The biggest fear is that terrorists could place a bomb in the cargo hold or wheel well, or they could hijack an aircraft just before takeoff. In 1986, terrorists dressed as security personnel crashed through the perimeter gate at the Karachi Airport and boarded a PanAm flight. The hijackers had planned to fly the aircraft to Israel and crash it into the Defense Ministry. Pakistani commandos subsequently stormed the plane, leading to a bloody assault that left 20 passengers dead.

Improving airport perimeter security seems simple compared with detecting underwear bombs. It is a matter of fences, cameras, and alarms—something we know how to do with readily available technologies.

Fences only delay determined attackers, providing an opportunity to reveal the breach and summon security personnel. Some airports use infrared or radar perimeter sensing systems, while others rely primarily on video surveillance. But cameras must be monitored. Some of these incidents show that the cameras worked, but security personnel did not take note.

Research shows that anyone observing multiple television screens can be effective only for a short time. However, technological solutions are available. Alarm systems may direct the attention of cameras and operators to possible intrusions. New smart cameras call attention to anomalous events—movement where there should be none, such as an individual coming over a fence—signaling the operator that something out of the ordinary is happening.

Airports could do more – at significant expense

The federal government could oblige the nation's airports to build more formidable barriers, cover them with more sophisticated alarms and cameras, and deploy more security personnel to increase the frequency of patrols and respond immediately to suspected intrusions. From the perspective of costs versus risks, it is not clear whether it makes sense to do this at all 450 commercial airports across the country.

Airports occupy large pieces of property. The perimeter of San Jose's airport, one of the country's smaller airports, is about five miles long. The perimeter of the Los Angeles airport is approximately ten miles long. Some airports are much larger. Dallas-Fort Worth occupies 17,207 acres and has a perimeter over 20 miles long, while Denver International occupies 34,000 acres, which means a perimeter more than 29 miles long. String all of the U.S. airport perimeters together, and we are approaching the length of the U.S. border with Mexico and security expenditures approaching a billion dollars.

The TSA is responsible for screening passengers. Airport perimeter security is a shared responsibility. Airports are responsible, with TSA ensuring that airports meet appropriate security levels. However, Congressional committees and the Government Accountability Office (GAO) have repeatedly criticized TSA's performance in exercising its oversight responsibilities. A 2009 GAO report, for example, pointed out that TSA had not conducted vulnerability assessments for 87 percent of the nation's approximately 450 commercial airports. Working with federal and local authorities, airports are supposed to complete these.

Persistent problems often have explanations other than bureaucratic sloth. The allegation that eight years after 9/11, those vulnerability assessments had not been done suggests underlying resistance. In this case, it comes from the airports, not the TSA. Airports resist vulnerability assessments because if they catalogue vulnerabilities, they must be remedied even if they are theoretical. If remedies are not implemented, the airport assumes a legal liability that trial lawyers could exploit if anything should happen.

It's a cost-versus-risk issue

Part of the resistance also comes from a perception of the threat. The perimeter breaches that have occurred in the United States thus far have been nuisances—embarrassing but not deadly, and not worth the millions of dollars for remedies.

"Show me a body count, and we'll build a fence," said one airport administrator, summing up a widespread attitude. It may sound callous, but if security is to be sensibly risk-based, then the risk must be shown. As risks are identified, they still must be prioritized for mitigation due to limited resources.

Security reportedly now accounts for 25 percent of current airport operating costs. Vulnerabilities exceed resources. Airports are strapped for funds, have limited sources of revenue, and are under pressure to address other issues. For example, recent shootings at airports have prompted

demands for an increased police presence in the publicly accessible parts of airport terminals.

What's more, there is no guarantee that increasing perimeter security will make a difference. New York and New Jersey's Port Authority reportedly spent $100 million on a perimeter security system, which did not prevent breaches at the JFK and Newark airports.

Enforcement can create adversaries

The TSA runs passenger screening, it does not run airport security. It can exhort airports to do more, it has enforcement authority, and it can impose modest fines on airports for security violations, although the absence of an agreed-upon vulnerability assessment makes it more difficult to demonstrate non-compliance. Theoretically, the TSA can even shut down a non-compliant airport—a "nuclear option" that risks public and political backlash.

Enforcing security measures creates an adversarial relationship. To a degree, this is true of all regulatory agencies—violations bring penalties. But it can have perverse effects in the area of security. Since it is difficult to empirically quantify the effects of specific security measures, compliance is reduced to doing precisely prescribed things—building a fence this many feet high, patrolling it so many times a day. It is mechanistic, rule-based rather than risk driven. The goal becomes adherence, not acceptance, which does not guarantee good security. Instead of being a partner, TSA becomes a meter maid handing out tickets for infractions.

Several imperfect options are on the table

This lesson must be kept in mind when allowing airports to take responsibility for passenger screening. As fiscal realities overshadow memories of 9/11, the pressure to reduce costs will increase. The amount currently spent by the federal government on passenger screening is already under assault. The federal government can retain oversight responsibility for ensuring performance, but enforcement could become increasingly illusory.

Continuing the current approach, TSA will retain oversight but lack practical means of enforcement. Airports will remain resistant to additional security expenditures. Breaches will occasionally occur, for which TSA will bear the brunt of the criticism. Absent a calamitous event, the state of perimeter security at airports will change very little.

Alternatively, Congress could push TSA to make airport perimeter a priority, giving it the authority and resources needed to bring about substantial improvements nationwide.

A less drastic course would recognize that the risks are real but modest. Unlike passenger screening—which must be the same at all airports because a breach at any airport exposes the entire system—the consequences of a perimeter security breach are confined to a specific airport. Egregious failures will result in more meaningful fines, while continued federal investment in research and TSA partnerships will gradually help airports reduce vulnerabilities.

ABOUT BRIAN MICHAEL JENKINS

Brian Michael Jenkins is an international authority on terrorism and sophisticated crime. He directs the Mineta Transportation Institute's (MTI) National Transportation Safety and Security Center, which focuses on research into protecting surface transportation against terrorist attacks. He is also a senior advisor to the president of RAND. From 1989-98, Mr. Jenkins was deputy chairman of Kroll Associates, an international investigative and consulting firm. Before that, he

was chairman of RAND's Political Science Department, where he also directed research on political violence. He has authored several books, chapters, and articles on counterterrorism, including *International Terrorism: A New Mode of Conflict* and *Will Terrorists Go Nuclear?* Most recently, he published *When Armies Divide*, a discussion about nuclear arms in the hands of rebelling armies. He also has been principal investigator for many peer-reviewed security-focused research reports for MTI. Go to transweb.sjsu.edu