AVIATION SECURITY INTERNATIONAL

www.asi-mag.com

THE GLOBAL JOURNAL OF AIRPORT & AIRLINE SECURITY

Daallo Airlines Bombing:

Somalia-based al-Shabaab targets aviation

ALSO:

SMART SECURITY

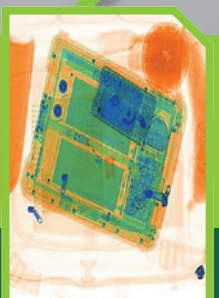
ADDRESSING THE INSIDER THREAT

THE SECURITY MANAUFACTURERS COALITION

SeMS

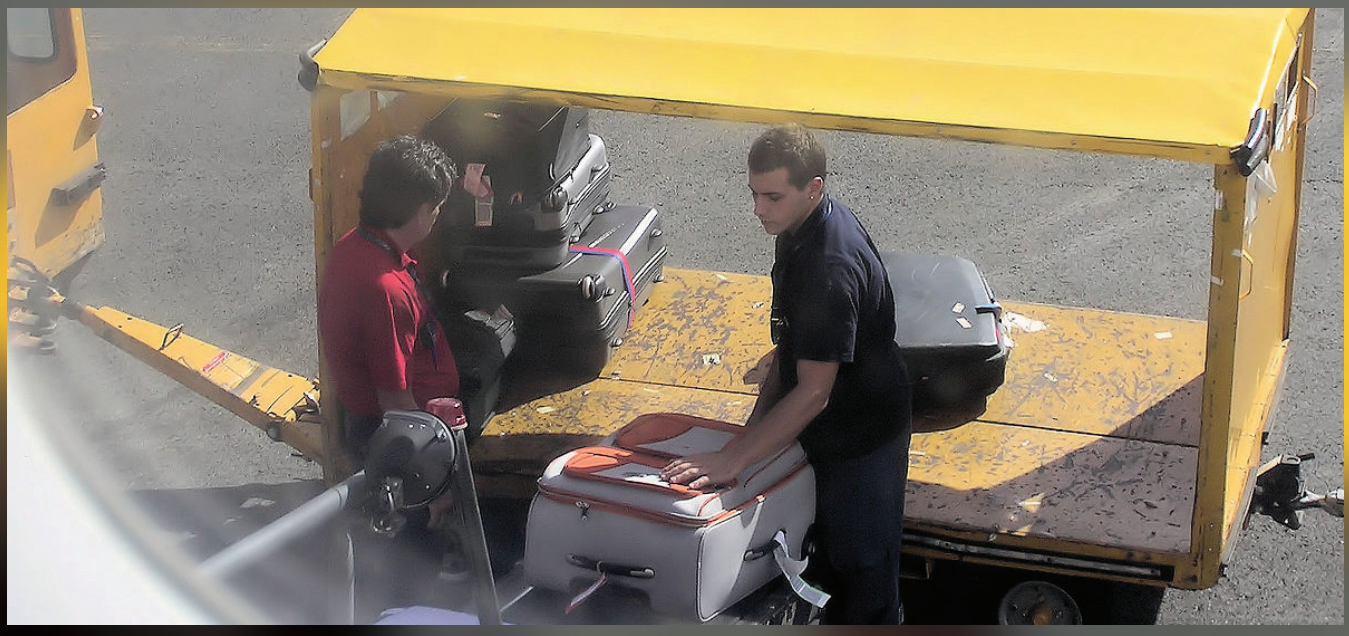
TERRORISM AND TOURISM

SCREENING LAPTOPS



INSIDER THREAT:

WHAT DO YOU DO WHEN THE CALL IS COMING FROM INSIDE THE HOUSE?



THE INSIDER THREAT IS NOT A NEW ONE TO THE AVIATION INDUSTRY, BUT ARE WE DOING ENOUGH TO COUNTER THIS ALL TOO FAMILIAR ENEMY? JEFFREY C. PRICE AND LORI BECKMAN DISCUSS THE IDEA OF A 'CULTURE OF SECURITY' AMONG AIRPORT STAFF AND ANALYSE HOW EFFECTIVE IDENTITY CARD MANAGEMENT AND EMPLOYEE SCREENING ON THE GROUND COULD REDUCE OUR VULNERABILITIES IN THE SKIES.

The 1979 horror movie *When a Stranger Calls* includes one of the most terrifying moments in movie history - when the victim discovers that the murderer who has been terrorising her all night is already in her house. Realising someone has penetrated our security measures, and is among us, is also one of the most terrifying forms of attack.

However, while one movie can represent the frightening nature of a threat, another may actually provide the answer. In the 1995 movie *Casino*, actor Robert DeNiro explains how casino security works:

> "In Vegas, everybody's gotta watch everybody else. Since the players are looking to beat the casino, the dealers are watching the players. The box men are watching the dealers. The floor men are watching the box men. The pit bosses are watching the floor men. The shift bosses are watching the pit bosses. The casino manager is watching the shift bosses. I'm watching the casino manager. And the eye-in-the-sky is watching us all."

Over the last few years we have seen a growing number of stories about aviation insiders carrying out illegal activities, from bag theft by airline and security personnel, to the transportation of narcotics and weapons by baggage handlers, screening personnel and, in some cases, even air marshals. But insider threats to aviation are not new.

The history of aviation terrorism is filled with numerous attacks where insiders either committed the attack, or were instrumental by providing access, materials or support. To a certain extent, even the 9/11 attacks had an insider element since the hijackers were trained by US flight training companies.

Drug smuggling in commercial and general aviation aircraft is a 46-year-old practice in the United States, ever since the passage of the Controlled Substances Act, which made many narcotics illegal to possess, use, distribute or transport. Aviation is still used to smuggle drugs, but also is a common method of transporting weapons, cash, victims of human trafficking, and stolen goods. Criminal acts however, present another challenge to aviation security, as someone who is already corrupt and using aviation to smuggle illicit goods may be more susceptible to being blackmailed into bringing more dangerous items on board, or may not even know what or whom they are smuggling. A baggage handler, who has been smuggling drugs on airliners for years, may not realise that the last suitcase they loaded on board did not contain drugs at all, but rather a bomb meant to bring down the flight.

Some of the most notorious terrorist attacks in the 1980s were facilitated or caused by aviation insiders. In the hijacking of TWA 847 in 1985, catering crews smuggled guns and grenades onto the flight so that the hijackers could clear security screening. In 1987, an airline employee who had just been fired brought down PSA Flight 1771; he was able to get a gun past the screening area because his airport access badge had not been confiscated and, at the time, employees were not required to go through screening when in possession of their identification badge. Then in 1994, a FedEx employee, who was also having personal issues, unsuccessfully attempted to seize control of a flight from his co-workers and pilot it into the ground.

Recent insider involvement in acts of aviation terrorism may include the bombing of two Russian airliners in 2004, where airline ticket agents were bribed as the suicide bombers did not have the proper identity documents, and, in 2015, the possible bombing of a Russian airliner over Egypt, in which a bomb may have been placed by an airline employee. Even the most recent incident, this February, involving Daallo Airlines in Somalia was probably effected using insiders.

While bringing bombs onto aircraft, or bypassing security measures to hijack an aircraft, or committing a crime, are traditional methods of insider attack, new threats are on the horizon. In 2011, a former British Airways worker was convicted on four counts of preparing acts of terrorism. Inspired by the preaching and teaching of al Qaeda's late propaganda minister, Anwar Al-Awlaki, Rajib Karim, a software engineer, told Al-Awlaki he had access to British Airways servers and could erase all data, causing massive flight disruptions and huge financial loss for the airline.

The solution to the insider threat lies in a layered system that includes creating a security culture, implementing effective employee credentialing standards, including methods for observing and assessing employee behaviour, and implementing random inspections to increase the likelihood that criminals or terrorists are caught.

Creating a security culture begins with embracing the concept of Security Management Systems (SeMS). SeMS begins with a security policy statement by management that supports the concept of *security-first* within all aspects of the airport or air carrier operation. Fortunately, SeMS and Safety Management Systems (SMS) are similar in structure and can work together so that the implementation of one eases the implementation of the other.

SeMS policy statements are reinforced by airport leaders' commitment to spend money on security risk assessments, mitigation efforts, assessment and audits of security processes, and security promotion strategies. Ultimately, the focus of SeMS is to make it not okay to let criminal activity take hold in the workplace, which, in turn, makes terrorist activity easier to spot.

"…the most recent incident, this February, involving Daallo Airlines in Somalia was probably effected using insiders…"

The proper implementation of SeMS requires a vulnerability assessment that goes beyond the traditional external threats, and focuses on internal threats, including cyberattack and employee computer access and usage, to the threats presented by those with complete access to the airport's secure areas. Security assurance programmes implement checks in the system to ensure that the existing vulnerabilities are addressed, and that processes to prevent attacks are working. Assurance programmes also keep an eye on developing threats, or emerging methods of bypassing security measures.

Creating a more robust security culture that includes insider threat management takes time and requires real action, such as workplace violence training that incorporates behaviour detection for all personnel, the promotion of security throughout all areas of the airport or air carrier operation, and educating the workforce on the real threats and their important role in stopping those threats being realised. In World War II, the poster 'Loose lips sink ships' reminded everyone to be careful about what they said and who they were saying it to. As citizens saw the damage caused by the failure to follow this tenet, the concept of not talking publicly about security, was reinforced and soon a security culture was built.

Building a security culture works on the 'broken windows' theory in law enforcement. Put simply, when a window is broken in a community, it should be immediately fixed, or else it will normalise the behaviour for others and more windows will be broken. From an aviation security perspective, if small violations, such as employees getting away with not always wearing their badge in secure areas, or lose control of escorted personnel in secure areas, it normalises the behaviour for others and soon more and more security rules are overlooked. Eventually, security becomes an afterthought, which creates fertile ground in which more serious criminal, and even terrorist, activity can take place. A security culture puts the DeNiro line from *Casino* into action at the airport level – everyone becomes a security asset.

Airport workers are extended an extraordinary amount of trust. Through their personnel identification badges, many employees are able to bypass passenger-screening checkpoints to access secure areas of the airport, including passenger aircraft. While airports and politicians continue to debate employee screening, the employee access identification badge remains the primary form of 'screening' for most airport workers. The security badging office provides another potential area for the insider to be able to carry out havoc upon the aviation system; a terrorist

Airports employ many low paid workers, such as cleaners, caterers and baggage handlers, where there is a high staff turnover rate.

Many airport employees have direct access to aircraft holds and areas which are not inspected by security personnel prior to a flight's departure.

with access to the airport's badging and physical access control system has the ability to grant access to themselves or accomplices, disarm doors, and silence door alarms or take them out of service.

The next layer in defeating the insider threat is knowing who to trust and ensuring those with the credentials to bypass elements of the system, can be trusted. This means effective background checks, periodic re-checks (the TSA is piloting the FBI Rap Back programme at several airports this year), effective security badging office oversight and ensuring the individuals in the security badging office itself, can be trusted.

All security badging office personnel (defined by the US TSA as Trusted Agents) should undergo background checks that are more extensive than normal employees, with lower tolerance for past transgressions. Computer tracking software must also be installed that assigns Trusted Agent access permissions by the exact level of access they need to complete their job duties, monitors system activity and will notify management of unusual activities by Trusted Agents or attempts to access areas they do not have authority to access.

Currently background checks for badge holders include a list of disqualifying crimes, and checks against national terrorist watch lists (called Security Threat Assessments or STAs in the US). Badge holders must be well trained on the proper use of their badge, such as secure storage when it's not in use, immediately reporting lost or stolen badges, challenging individuals without proper identification and proper escort procedures where applicable.

Upon completion of the background check, badge holders must be continually vetted to ensure they have not been subsequently arrested for criminal activity. In the US, STAs are perpetual and fingerprint-based criminal history record checks which must be conducted for every badge renewal. Company managers (known as Authorised Signatories), who approve which of their employees are to obtain badges, must be required to report any employee who has been terminated, resigns, or has been convicted of a disqualifying crime, immediately, to the security badging office – and then make every attempt to obtain the badge. The security badging office must then immediately invalidate the badge holder's access in the system. Airports and air carriers must have a process in place so that ideally, a badge can be cancelled out of the system 24/7, and the appropriate security and law enforcement immediately notified if necessary.

> "...conducting random inspections only part of the time, can be just as effective as inspecting all personnel..."

With the recent news stories of smuggled goods by airline employees at US airports, some politicians in the US have been calling for 100% screening of all employees. While this practice is commonplace at some airports throughout the world, most US airport checkpoints were not designed to handle the employee throughput traffic. Also, most US airports are designed to accept employees arriving at the airport by car, not public transportation, so separate employee parking lots were constructed and arrangements made so that much of the employee population could access the security areas of the airport, without going through screening.

Some airports, such as Miami, Orlando, and Atlanta/Hartsfield International have established full screening and/or property inspections for their employees. In the US, the Aviation Security Advisory Committee recommended that airports implement random employee inspections. The US Transportation Security Administration has issued additional rules to US airports that are currently protected as sensitive security information), but TSA has said publicly that the agency may be moving towards making employee inspections mandatory.

Employee screening and employee inspections are two different processes. Screening is considered to be the same process which passengers undergo, using the same technologies and procedures, whilst inspections are manual searches, usually involving a physical hand search of employee belongings, and using hand wands or explosive trace detectors for the identification of weapons and explosive materials. Some studies have revealed that conducting random inspections only part of the time, can be just as effective as inspecting all personnel.

If airport operators want to avoid the massive costs and considerable operational inefficiencies associated with 100% employee screening, at a minimum, employee inspections should become the norm at all airports. In the US, if employee inspections are mandated, the airport operator will likely get stuck with most of the bill, but it's a matter of *pay me now or pay me later*. Airports can either implement employee inspection programs at a lower cost now, or wait until an insider commits a devastating attack on aviation (again), and then pay the much higher costs of 100% employee screening.

Employee inspections can be carried out by unarmed security personnel, supported with armed law enforcement when necessary. Fixed-position employee inspection stations should be located where employee throughput is highest. US airports already have been directed to limit the number of security area access points, which is a basic security principle. Fixed-positions work well when there are fewer options for employees to go through another door that bypasses the inspection station. Fixed-position stations can be staffed at random times, depending on the threat level.

Mobile inspection teams can also be established, rotating to various

employee access doors for periods of times. Employees will often quickly spread the word about which inspection stations are in operation so that their co-workers can avoid the area, so random stations are only effective for a limited period of time. Getting employees to not tell each other which doors to avoid due to a mobile inspection stations can become a goal of the security promotion programme, but will always occur at some level.

Inspections of vehicles and personnel should always be carried out at any staffed vehicle access gate. Methods for inspecting catered goods, vendor deliveries and contractors accessing the airfield should be in place (they are presently mandatory in the US). However, there must also be some flexibility in the application of the rules for airport operations, police, fire, emergency medical, air traffic control maintenance personnel, and others whose work could be significantly impacted by continuous slowdowns at inspection stations. These individuals may be subjected to higher levels of background checks as a way to offset their ability to bypass certain inspection requirements.

Employee inspection personnel should receive hands-on training on how to inspect common employee belongings, such as purses, backpacks and laptop bags, and how to conduct a hand wand or, if called for, a pat-down inspection. Employee inspection personnel should also be trained in the identification of weapons, explosives and drugs, and how to find hidden pockets in bags. Standard suspicious awareness and behaviour detection training should also be a part of their training curriculum; while there may not have been explosives in a given employee's laptop, but there was a large sum of cash or a few dozen mobile phones instead, this should immediately send red flags to the security personnel, and law enforcement should be contacted.

The insider threat to aviation has always been one of the most insidious and, frankly, scary types of threats. The access provided to airport and airline workers bypasses most of the security systems that are put into place to prevent passengers, and others, from bombing, hijacking, or otherwise attacking the system. An airport identification badge is quite plainly, the key to the house. However, implementing Security Management Systems helps to operate a tight ship when it comes to the credentialing of personnel, beginning with the security badging office.

Many airports have begun transitioning away from traditional badging systems and are implementing identity management systems, which can track an individual identity no matter who their employer is, or was, with the integration of analytics that can track behaviours. Irregular behaviours cause an alert that can be further researched and observed by a trusted individual. Conducting random inspections of employees can also greatly reduce the chances that the attack will be coming from inside the house. ■

Jeffrey C. Price is the lead author of 'Practical Aviation Security: Predicting and Preventing Future Threats', a professor at the Metropolitan State University of Denver, and the owner of Leading Edge Strategies. He can be reached at pricej@msudenver.edu

Lori Beckman, A.A.E., ACE-Security, is president of Aviation Security Consulting, Inc. She may be reached at lbeckman@avsec.biz