

# God in the Machine: the human factor in Aviation Securi...

Author : admin

Published: September 8, 2010, 7:48 pm

---

by Professor Francis Spranza for AviationNews.us

## God in the Machine: the human factor in Aviation Security

If there is one lesson we in the industry should take away from the events of the Christmas Holiday of 2009 involving Northwest Airlines Flight 253 it is that no matter how advanced the technical aspects of aviation security become, the true bottom line of aviation security remains the Human Factor.

Umar Farouk Abdulmatallab, was easily able to circumvent the current generation of x-ray scanners at Schipol Airport which are designed to detect metal objects. Although technology offers high intensity microwave scanners, known as millimeter wave scanners, (aka. Whole body imaging devices such as [L3's ProVision](#)), where clothing and other organic materials are translucent, the MWS deployed at Schipol Airport is of a generation less powerful. The selection choice for Schipol was made based on health concerns and privacy issues of travelers, both understandable constraints.

In the case of Sunday's flight, cabin crew and passengers onboard Flight 253 – again from Amsterdam to Detroit - came together in response to preempt what may have been a potentially volatile act of unlawful interference. Although innocent of wrongdoing, the suspicious activity of the unnamed Nigerian businessman prompted a human response in the protection of the aircraft, its passengers and crew.

Earlier in the year, on 26/27 September 2009, retired Israeli police officer Daniel Sharon was traveling on Delta flight 086 from New York to Tel Aviv. As he waited to board the flight at JFK, cognizant of those around him, Sharon observed a woman whose behavior appeared out of the norm. His suspicions were triggered by both her conversation and physical mannerisms. Having to subdue the woman in mid flight, Ret. Officer Sharon's actions were lauded by the Delta station manager both for preventing a major incident and protecting the airline's reputation to say nothing of the financial cost which would have been incurred in undertaking unscheduled emergency landing.

In our Post 9/11 world we have come to rely on a host of scanners, sniffers, x-ray machines, swab devices and computerized detection systems to ensure the safety and security of passengers, crew and equipment. Our faith in deus ex machina, (god from a machine) has prompted us to all but ignore the human security machine. Too often airports and CAA agencies invest heavily in high tech equipment ranging from perimeter and terminal CCTV to security checkpoint screening machines, cargo x-ray units and computerized access systems – all of which are completely justified in today's modern world, while having a security force whose standards, practices and evaluations are virtually non-existent (save for paper for "inspection" purposes).

As the author's personal experiences have shown, is it no wonder that contraband is freely passed through chain link fences in full view, or that undocumented travelers are able to easily board flights with little more than a "donation" to the proper immigration officer at their point of origin, regardless of the sophisticated CCTV units and MIS systems in place? Or, that passengers are instructed to put open liquids ( in this case a cup of coffee) on the x-ray screener belt so it can spill, short the machine's electronics and result in hand searches of all passengers for months while a replacement machine is sought out? Or, the security officer who, while wandng a passenger hears the alarm beep as the wand passes over the passenger and ignoring the tone while failing to clear the alarm, simply says, "Ok, move on". Or, that many airport security personnel lack even the most basic AVSEC training found in the [ICAO Basic AVSEC&nbsp;ASTP](#) or similar [commercially available training](#). Though certainly not the case across the board, none of us can deny incidents such as these occur far more frequently than we would like to admit.

---

It would appear that airport decision-makers and administrators have come to place the value of technology above that of the basics -- old fashioned security force personnel selection, training, and evaluation. If there is one thing we must come to understand, one lesson airport management, airline operators and security administrators must realize is that you cannot replace basic human skills with any amount of technology. Technology is a tool to supplement the basic human skills acquired through proper training, skill practice and supervisor evaluations.

Administrators, planners and financial officers **MUST** make the investment in personnel selection, initial and mandatory re-training as well as providing for outside consultants to review, revise and maintain cutting edge techniques in continuing education – such as interactive distance learning, full scale scenarios and daily systems tests.

Not being academics, trainers or familiar with the contents of a comprehensive aviation security training program, one might ask: what should such a curriculum entail? The chart shown below indicates course title, applicable end user and the recommended number of instructional hours for each program area.

---

---

Training Program  
User Base  
Suggested Duration

---

---

Basic AVSEC  
AIRPORT SECURITY  
80 instructional hours

---

Supervisor Basic  
AIRPORT / AIRLINE  
40 instructional hours

---

Supervisor Advanced  
AIRPORT/AIRLINE  
56 instructional hours

---

Checkpoint Screener Certification  
AIRPORT/ CONTRACT  
160 instructional hours w/ OJT

---

Profiling  
AIRPORT/CABIN CREW  
40 instructional hours

---

---

CCTV Operator Certification  
AIRPORT/CONTRACT  
24 instructional hours

---

CQT training  
AIRPORT/ AIRLINE FSM/GSC  
32 instructional hours

---

FSM/GSC Certification  
AIRLINE  
40 instructional hours

---

Cargo Security  
Hazardous Materials & Dangerous Goods  
AIRPORT/AIRLINE/CONTRACT  
56 instructional hours

---

Training for Trainers  
AIRPORT/AIRLINE  
56 instructional hours  
Source: <http://icao.int/td/>

Classroom training alone is but one part of the effectiveness of personnel. They need Training, Practice and Evaluation. Skills learned must be regularly practiced, evaluated and documented in order for the learning experience to be truly effective and for personnel to perform as expected during potential or actual emergency situations. When taken together, these elements ensure a cohesive and comprehensive airport team response. Airport and Airline security policy and procedures must contain provisions clearly stating that the AVSEC practice and evaluation environment MUST:

- a. be as realistic as possible.
- b. be conducted on a no-notice basis
- c. represent real world scenarios
- d. reflect the creativity of potential perpetrators
- e. contain an element of feedback to the field personnel

The airline industry as whole has come to rely on technology developed after the fact to thwart a variety of situations which could result in one or another acts of unlawful interference. As such, it appears we have forgotten the basics of Proactive Response. Take for example, the restrictions placed on carry on liquids after the London incident, or proliferation of metal detectors following 9/11, or shoe inspections following the Richard Reid incident.

Technology has its place, and demands proper research and development funding, testing and field deployment. However, all the technology imagined by man, cannot replace a well-trained and properly motivated security officer.

Airport and Airline administrators must rethink their approach and take a proactive stance, avoiding "public theater" and focusing on a multi-level network of intelligence, pro-active planning, training and exercises designed not to respond to a previous incident, but rather to anticipate any future terrorist plans.

AviationNews.us note: Professor Francis Spranza is the owner of: [Spranza](#) and [Avsec-Center](#)