AVIATION security international

The Journal of Airport & Airline Security www.asi-mag.com

April 2007 : Volume 13 Issue 2

Hijacked From Tirana:

an interview with the Turkish Airlines crew

Securing Airside Deliveries
Screener Training Software
Hijack Victim Experience
Muslim Passengers
Biometrics

If At First You Don't Succeed...

try, try, and try again

by Philip Baum

When Ramzi Youssef failed to bring down the Twin Towers in February 1993, a decision was made: to try again, yet using different means. In 2001, more than eight years later, al Qaeda succeeded using commercial airliners as weapons of mass destruction.

In 1995 Ramzi Youssef failed to realise Oplan Bojinka and destroy multiple trans-Pacific flights utilising liquid explosive devices. Eleven years later, in 2006, like-thinking individuals failed again, but this time targeting trans-Atlantic aircraft. Multiple flights destined for, or perhaps departing from the United States will be targeted in the future; it may be some time off, but it will already be being planned for and time is not, from their perspective, of the essence.

Al Qaeda's trademarks are multiple attacks and undetectable weapons. In 2001 they used boxcutters, at the time not considered a threat; by 2006 they'd returned to the concept of liquid explosives, but now to be carried and detonated by suicide bombers.

Reactive, as always, we have implemented a raft of security measures designed to counter the modus operandi of the past.

It is perfectly understandable that short-term remedies to plots, be they failed or successful, may include the banning or limiting of specific items or substances associated with the identified attack methodology. Indeed it is now unlikely that an attempt will be made to target aircraft using liquid explosives carried by passengers through a security checkpoint where LAGs (liquids, aerosols and gels) are limited; there is too much of a risk of being caught and an organisation such as al Qaeda doesn't wish to take its chances; it wants guaranteed success once the operation is underway. Notably, both in 1995 and in 2006, the operations were prevented at the planning stage; no actual attempt was ever made to infiltrate devices onto aircraft on the day of the "main event", albeit a test device had detonated on board a Philippine Airlines flight in December 2004.

What is also of significance in the timing of the previous attempts and actual successes is that recent terror extravaganzas have been scheduled on days of no or little significance (unless one considers the numbers "nine eleven" to have symbolic importance). So, whilst we make proclamations about "increased threat" levels associated with highly publicised events or inter-governmental meetings, the actual evidence would suggest that, if anything, the threat is either diminished as the increased security presence will simply persuade the terrorist to attack on a different day or plays a hand in changing the location of the attack due to resources being skewed in one direction. After all, why attack when one's chances of being detected are at their highest?

Take the London bombings of 2005 as an example. The timing may have been significant inasmuch as the G8 leaders were gathered in the United Kingdom for a summit. As a result much of the security services focus was concentrated on Scotland, where the leaders were gathered, rather than in London where the attack took place. (Even we had run an article about securing the G8 Summit in the preceding months and the entire article focussed on countermeasures "north of the border".) The fact that the attack took place the day after London had won the bid to host the 2012 Olympic Games was probably merely fortuitous for the organising cell as it is highly unlikely that the event was planned the day before and, in respect of pre-planning, Paris was the favourite to win the bid.

> "...does the system as a whole actually do what is it supposed to do..."

There are phrases that stick in one's mind that I have heard at industry events and subsequently quoted in previous editorials. For example, you may recall my referring to Sidney Chau's message to screeners in Hong Kong to "maintain a sense of crisis 24/7" – a worthy ideal. I now have a new one to add to the list. At the recent Asia Pacific Aviation Security Summit held in Melbourne, Australia, Chameleon's Amotz Brandes stated, in questioning the value of the various American colour-coded threat levels, that "there is no such thing as an increased threat; there is just a threat". And how right he is.

There is an important public perception that aviation is considerably more secure nowadays that it was pre-10th August 2006, which was already more secure than it was pre-Shoebomber and pre-9/11. It may be such a perception that has brought about attacks against other modes of transportation. It is easier by far to target the Madrid rail network or London Underground...

But, aviation will long remain the crème de la crème of targets due to a successful attack's impact around the globe. More importantly, however, to date, the al Qaeda network has failed to realise its desire to destroy multiple airliners carrying significant

loads of multi-national passengers to the United States. It will try, try, and try again.

It is often said that the best security programmes are those that are re-written from scratch. They are like suits. For quality, one goes to a tailor who will design, cut and fit the product until the customer is satisfied. On the other hand, if one desires something cheap yet acceptable to the masses, one can buy an off-the-shelf product and accept its limitations. By taking "model" programmes, cutting and pasting seemingly pertinent clauses into a document, one meets the core international or national requirements, yet does not necessarily have a quality programme.

Meeting the international requirements stipulated by ICAO's Annex 17 to the Chicago Convention, ECACs Doc 30 or other legislation may be laudable, but is it effective in meeting the challenges of the threat we face 24/7 in the 21st Century? I think not.

Standardised testing of screeners may be "fair" for the operatives themselves, but not for society as a whole. Take Threat Image Projection (TIP) as an example. We test our X-ray operators with concealments that they should be able to detect rather than testing all of our screeners with terrorist modus operandi that they have not even considered. Where's the logic in that? Surely, if we are to test the system, as we should be doing on a daily basis, we should be doing so as if we want to penetrate the system as a whole?

> "...the reason we don't pose the question is because we are afraid of the answer..."

For far too many airports, airlines and even regulators, aviation security has become one big tick-box (check-box) exercise. Do we have an airport security programme? Do we test our screeners? Do we effect background checks? Do we screen all checked luggage? Do we issue vehicle passes to airside vehicles? And so on... Yet how often do we ask ourselves the question, "does the system as a whole actually do what is it supposed to do and prevent all acts of unlawful interference with civil aviation"?

I submit that the reason we don't pose the question is because we are afraid of the answer and that, consequently, there is a serious need for some fresh thinking about our global approach to tackling the problem. That means going back to basics and questioning the efficacy of every element of the defence strategy. It means there are no "givens", no "that's the way we do things", and no "bolt-on solutions".

Terrorists are a little like spiders. They lurk in the shadows, they creep quietly and are never heard, they weave webs to snare their enemy, they are small in size yet frighten the masses, their elite forces have a deadly bite and, when they fall, they try, try, and try again.

Indeed, the saying "if at first you don't succeed, try, try and try again", is attributed to Scotland's Robert the Bruce who, whilst hiding in a cave contemplating his future, was inspired to fight on for Scottish independence from England when he saw a spider continually fall, yet repeatedly try again to achieve its goal.

Yet, like spiders, the terrorist under surveillance, whilst unnerving, is defeatable. Unlike spiders, today's terrorist may change its tactics, whilst maintaining a common goal. In response we need fluid tactics, unconstrained by standard response formulae, political correctness and dumbed-down methodologies...