

EMPLOYEE BACKGROUND CHECKS:

AN ID PASS TO THE STERILE ZONE

Allegedly, although mired in much controversy and conspiracy, the most notorious attack perpetrated by an aviation employee with access to airside operations is that of Abdelbaset Ali al-Megrahi, convicted of the bombing of Pan Am flight 103 over Lockerbie in 1988. He was the head of security for Libyan Arab Airlines (and an alleged Libyan intelligence agent) and was found guilty of placing the bomb in a suitcase at Malta's Luqa Airport. This, however, is a rare case involving state-sponsored terrorism against civil aviation, and involving a very senior airline official.

Following 9/11, governments around the world pledged to make airports more secure. The stringent security

measures and advanced technologies implemented over the past decade are redundant if those we entrust with keeping our airports and airlines operational are able to slip through the net unchecked. Therefore, the enhanced security implemented in many countries included measures to ensure all of those working in sensitive areas – mainly airside - at airports were thoroughly checked for criminal records and other risk-related activities. After all, if the 9/11 hijackers were able to infiltrate flight training schools, the next round of terrorists would surely have airports and airlines in their sight for infiltration. It is not just the terrorist threat that is a major issue when recruiting aviation staff to security sensitive positions; more common is the threat from gangs and networks involved in drug, arms and

human trafficking, money laundering and theft amongst other illegal and violent activities.

Background Check Procedures

In the United States, in the wake of 9/11, hundreds of airport workers were arrested and many indicted nationwide for immigration offences. The raids attracted negative publicity for mainly focussing on Hispanic workers, many with families and not all of whom were still employed at airports. The then US Attorney Bob Conrad said: "Terrorists could use the fact that workers are illegal aliens to blackmail them into assisting the effort to sabotage a plane. That's the concern that motivated this investigation. This is a preventative effort."

With criminal gangs operating airside at many of the world's larger airports, developing a system of evaluating who we should issue airport ID to is a major challenge. It's not only the initial issuance of the pass, but also the continued surveillance of those we employ. How can we address the issue, without impinging upon personal privacy, and ensure that those operating airside are honest law-abiding citizens? Anna Costin reports.

The Transportation Security Administration (TSA), set up following 9/11, is responsible for vetting airport staff working in security sensitive areas. After vetting, it issues Secure Identification Display Area Badges (SIDA) to staff working in secure areas beyond alarmed doors where they can access the flight line, ramp and aircraft. It issues active sterile area badges to staff, after vetting, working beyond the passenger screening checkpoint but inside the terminal area. From October 2007, TSA began requiring airports to receive a favourable security threat assessment for all staff before issuing them with badges. Prior to that, the airport itself conducted a background check, issued a badge and then submitted new employee data to the TSA, who only then carried out a security threat assessment. Now, when an individual is hired to work at an airport, the airport sends their background information to the Airport Association of Airport Executives (AAAE) Transportation Security Clearinghouse. AAAE sends the information onto the TSA. The TSA's security threat assessment checks the person against 10 databases including the Terrorist Screening Database (TSDB) and also determines whether there are any outstanding immigration, terrorist or federal open warrants pending against them. This assessment usually takes 72 hours to complete. At the same time, the airport conducts a background investigation – which must cover at least the previous 10 years if staff are to be deployed to

secure areas - checking the individual – including their fingerprints – against the FBI database for any of the 28 crimes that would disqualify them from employment. These crimes include forgery, unlawful possession of a weapon or explosive material, interfering with a flight crew or flight attendants, certain violent crimes causing bodily injury or death, treason, extortion, arson and conspiracy. For the most sensitive positions the process

"...Project Spawn found that security had been compromised by suspected hundreds of workers who have used their security clearances to smuggle drugs and people into Canada..."

can take anywhere between 27 to 106 days to complete. Drug screening is also conducted. From September 2005, TSA started using a system of perpetual name-based vetting of all TSA, airline, airport and airport vendor employees and contractors; each time a name is added to any one

of the databases all employees who currently have access to secure areas are immediately checked against the new information.

More than 1000 applicants are vetted each week. If an applicant returns as a possible match with information contained in the databases they are checked against, they undergo further analysis. If after that further analysis they are deemed to pose a security threat, information about them is sent to law enforcement or intelligence agencies. These agencies determine whether the individual's identity can be verified and whether they continue to pose a threat and they notify TSA, which in turn notifies airports or airlines when an employee's access to secure areas must be denied or withdrawn. In order to access sterile areas, individuals who do not possess SIDA badges, including airline and airport personnel, must pass through the security screening checkpoint; the same physical screening process that passengers must pass through before boarding aircraft.

In the UK, since 2003, all individuals working airside have been checked against UK criminal records, but offences overseas are not covered. This was brought to light in May 2008 when the BBC reported that foreign workers employed airside at UK airports are not subject to full criminal records checks. A Department for Transport spokesman in response to the BBC report said the terrorist threat to aviation from airside workers is "fundamentally addressed by physical security measures, for all



staff, every day". He added: "In addition to physical security, we run a counter-terrorist check, which is far more detailed than a criminal record check, for all airside workers engaged in security roles". In June 2009 the government scrapped its plans to force airside workers at airports to carry identity cards before they could be issued with security passes for the airport.

Plans for identity cards for all UK residents and nationals have since been scrapped.

In Australia, airport staff have to submit to a background check every two years.

Paul Jones, security manager for Qantas, believes this should be more frequent and

"...calling herself the Lyrical Terrorist, she wrote poems about terrorism and martyrdom and had a well stocked library of documents likely to be used for terrorism..."

that staff should also have to declare when they have been charged with a criminal offence, not just when they have been convicted. In February 2010, the Sydney Morning Herald reported that airport and maritime port workers could face mandatory fingerprinting. The agency that checks the backgrounds of workers with access to sensitive sections of ports and airports, CrimTrac, told a parliamentary inquiry that name-based background checks used now can be bypassed with assumed identities. CrimTrac advises that all employees undergo fingerprint-based identity checks for the new Aviation Security Identification Card or Maritime Security Identification Card systems. The inquiry follows a report in 2009 that criminal gangs had infiltrated the country's ports and a leaked 2005 report that drugs smugglers were working at Sydney Airport.

Notable incidents

It appears that despite more stringent post 9/11 employee background

checks, illegal activities involving airport workers have continued to take place around the world.

Canada

In 2008, the Royal Canadian Mounted Police (RCMP) published their Project Spawn report - a two-year inquiry into hundreds of investigations between 2005 and 2007 at the country's eight largest airports. It found that security had been compromised by suspected hundreds of workers who have used their security clearances to smuggle drugs and people into Canada. The three airports bearing the brunt of these infiltrations were Toronto's Pearson International Airport, Montreal's Trudeau International Airport and Vancouver International Airport. Not all cases led to charges and convictions and the RCMP said that 68 of the problem employees were still working at airports at the conclusion of the inquiry.

Federal laws prevent Transport Canada, responsible for the employment and screening of airport workers, the



Canada Border Service Agency and the RCMP from sharing information on employees, and a criminal record does not automatically preclude getting an airport job. Senator Colin Kenny, Chair of the national-security committee, says: "where you have fertile ground for organised crime, you also have fertile ground for terrorists." Transport Canada said it was developing a "comprehensive response" to the issues raised. Project Spawn also flagged around 1000 outsiders intent on infiltrating airports to facilitate crime. The report details these as agents of 58 crime groups, working at corrupting existing employees or by placing criminal associates into the airport workforce.

In 2006, a crackdown against mafia families unveiled the extent to which they had infiltrated Trudeau Airport, using airline employees, a catering company and baggage handlers to import cocaine. They also relied on a corrupt customs agent who facilitated the passage of drugs couriers through the airport.

UK

In February 2002, £4.5 million was stolen in various currencies from British Airways during a robbery at Heathrow Airport. In 2006, a baggage handler at the airport was one of several men convicted over the heist.

In 2007, 23-year-old Samina Malik became the first woman to be convicted under the UK's 2000 Terrorism Act for possessing records likely to be used for terrorism. She was an airside retail employee at Heathrow Airport. Calling herself the Lyrical Terrorist (presumably based on the 'lyrical gangster' coined in a 1994 Ini Kazome song), she wrote poems about terrorism and martyrdom and had a well stocked library of documents likely to be used for terrorism. In 2008 her conviction was quashed by the appeal court. Was there anything obvious or notable in Malik's background or profile that would have alerted authorities to her activities? It seems unlikely. Her trial judge described her as an enigma. Malik described her poetry as meaningless and that her words had been taken out of context.

It emerged in January 2008, one month after her conviction, that she had been in e-mail contact with Sohail Qureshi who was jailed that month for four and a half years for preparing to engage in terrorism. She advised him on the levels of security at Heathrow Airport shortly before he travelled to Heathrow with the purpose of flying to Pakistan and then joining a terrorist group. This fact was kept from the jury during her trial for fear of it prejudicing Qureshi's case.

It is not just airside personnel who should be subject to stringent background and ongoing security checks, but airline personnel too. In March 2010, a British Airways software developer based at the company's

Newcastle offices was arrested and charged with preparing acts of suicide terrorism. Bangladeshi born, Rajib Karim, 31, is due to go on trial in January. It is alleged he assisted in the commission of terrorist acts by providing information on topics such as liquid allowances on planes, airport security and scanners and immigration questions to travellers. He is also alleged to have provided details on BA computers and their vulnerability to a physical or internal systems attack to inflict financial loss. Information was also alleged to have been provided on the opportunity to obtain cabin crew training, information, experience – by attempting to volunteer for temporary cabin crew training

ISRAELI TRANSPORTATION SECURITY SOLUTIONS DELEGATION

21-27 February 2011



REGISTER ONLINE AT WWW.AVSEC.COM

Programme includes:

Ben Gurion Airport	Eilat Seaport	Taba Crossing
		
Old City of Jerusalem	Security Mindset	Simulations
		
Israel Railways	Technology Showcase	
		

Organised by:



Sponsored by:



Run in conjunction with:






Abdelbaset Ali al-Megrahi, convicted of the bombing of Pan Am flight 103 over Lockerbie in 1988, was the head of security for Libyan Arab Airlines

provided by BA to cover strike action by permanent cabin crew - and aircraft access and "inside knowledge". He is also accused of giving advice about working for BA and obtaining a British passport. BA said Mr Karim had not received aircrew training as he did not meet the criteria.

Venezuela

In 2002 global intelligence company Stratfor reported that a crime ring was working at Caracas' Simon Bolivar Airport in Venezuela, kidnapping and robbing foreign travellers, with the help of corrupt immigration

officials who pass on the address of where the traveller is staying to their accomplices in the main concourse who then follow the unsuspecting individuals.

Conclusion

Not all individuals engaged in crime or terrorism have a criminal record and are therefore identifiable. Some airside workers engaged in illegal activities may become involved in such behaviour after commencing their employment and passing background checks. The issue of foreign airside workers and ex-patriots

returning home to work in airside roles after years abroad needs to be better addressed as comprehensive checks cannot always be undertaken on such individuals. If they are not to be automatically excluded from these roles, law enforcement agencies must co-operate to a greater extent internationally; this is a matter that needs to be driven at the inter-governmental level.

Money is as ever a pertinent issue; subjecting every airport and airline worker to an extensive and perpetual (e.g. annual, bi-annual) check, and, for those working airside, subjecting them to physical screening whenever they access areas beyond the checkpoint, would not be economically feasible – the cost would outweigh the threat. Another money-related issue is that many airport employees working in sensitive positions of trust e.g. security screeners and baggage handlers, are low paid, and prone to low morale. Turnover in these jobs is high and some of these workers could potentially be vulnerable to being bribed by criminal or terrorist gangs.

Airport and airline employees have a right to privacy. Unauthorised background checks and / or surveillance would be unlawful, and also unethical. The need for aviation security has to be balanced against the right to privacy and data protection.

Like all areas of aviation security, employee background checks need to be as uniform as possible internationally in order to be effective. This involves multiple jurisdictions and policies. There is no failsafe method of screening, both initially and repeatedly, employees working in secure airport areas. It is impossible to predict whether an employee will become involved in illicit activities either inside or outside of work. But by completing as thorough a check as practical, repeating that at reasonable intervals, ensuring security procedures are adhered to, airport surveillance is optimal and staff are well paid, well trained and highly motivated, authorities can justifiably say they are doing all they can to keep airports, aircraft, passengers and staff as secure as possible. ■

"...a crime ring was working at Caracas' Simon Bolivar Airport in Venezuela, kidnapping and robbing foreign travellers, with the help of corrupt immigration officials who pass on the address of where the traveller is staying..."