METROJET FLIGHT KGL9268: HIGHLIGHTING THE INSIDER THREAT

By Philip Baum

I had the privilege of chairing the session on the 'Insider Threat' at AVSEC World 2015 (the annual global aviation security conference, nowadays co-hosted by the International Air Transport Association, Airports Council International and International Civil Aviation Organisation) held in Dublin. During the Q&A session, one airport delegate questioned whether we were placing excessive focus on the insider threat, and asking why, if we were as vulnerable to attack as so many of us were intimating, the industry had not suffered a significant attack as a result. Well, perhaps, we now have.

One month on from the loss of Metrojet flight KGL9268, 23 minutes after its departure from Sharm el-Sheikh bound for St. Petersburg, all the indicators suggest that the explosion that took place was caused by an improvised explosive device. If it is eventually confirmed that it was a bomb, Islamic State in the Sinai Peninsular/Province are the most likely perpetrators of the attack.

As is commonplace in the aftermath of a tragedy, there is considerable focus on the security measures that were in place at the point of departure. The media is awash with stories from visitors to the Red Sea resort keen to relate their accounts of the inadequate security processes they had witnessed. Whilst some of them are shocking, they are not surprising. The harsh reality is that whichever airport the doomed flight had departed from, there would be similar stories told. Sharm el-Sheikh may well not be an example of best security practice, but it does not stand alone.

The wreckage of Metrojet flight KGL9268 in the Sinai (Credit: Russian Ministry for Emergency Situations)

"…let's remind ourselves of the findings of this year's US Government Accountability Office's report into screening at American airports – in 67 out of 70 tests, inspectors were able to infiltrate prohibited items, including dummy IEDs, through security checkpoints. That's a 95% failure rate…"

Many have been quick to criticise the passenger screening process – being the most visible element of the security infrastructure of an airport – and government inspectors have rushed to the scene to evaluate the standards in place. I'm sure that there is room for improvement, but let's remind ourselves of the findings of this year's US Government Accountability Office's report into screening at American airports – in 67 out of 70 tests, inspectors were able to infiltrate prohibited items, including dummy IEDs, through security checkpoints. That's a 95% failure rate. Furthermore, government tests, wherever they are conducted around the world, have to be detectable by the screeners – to be fair tests; terrorists attempt to conceal, or infiltrate, devices in ways that are not detectable.

Away from airports, even the most secure facilities, such as prisons, cannot ensure the detection of all prohibited items, despite there being next to no limit on the amount of time one spends screening prisoners, visitors and staff and no customer service issues to worry about.

The images we now see of 'enhanced' screening in process in Sharm el-Sheikh do little to inspire confidence in the security professional, although I accept that they may reassure the travelling public. Whilst the industry is generally supportive of passenger differentiation – using a common-sense, risk-based approach to security – the sight of everybody undergoing a pat-down search, with zero consideration as to the passenger's profile, is illustrative of the theatrical approach the world has taken to screening.

Over the last few days we have heard continual reference to the word 'compliance' as if that was in itself the goal. Compliance is the bare minimum we should be achieving and somehow we have to create an operating environment where we aim to excel and exceed baseline levels. Ultimately, of course, it all boils down to money and whether airports and airlines are prepared to make the necessary investment in human life.

In far too many countries around the world, aviation security personnel are poorly paid and struggle to support their families. Other security agencies operating at airports – customs, immigration, quarantine – all tend to pay more and hire staff of a better calibre than those tasked with pre-flight checks.

Given the threats that exit, this is no longer tenable. How can we expect excellence in security controls from people who are lacking in education and motivation? As is often said, if you pay peanuts, you get monkeys.

In many airports in the developing world, corruption is rife and bribes are readily accepted; most financial exchanges are made for a 'service' by which one is expedited through the airport process, rather than to bypass security controls, but a £10 note - or $10 bill - has a lot of purchasing power. The industry has failed to address this concern adequately. In certain countries, bribery is endemic and part and parcel of daily life, so it is incumbent upon operators to aggressively tackle the problem – encouraging reporting, banning staff from carrying cash (so that periodic spot checks can be effected), and making the acceptance of bribes – or, indeed, payment for any 'extra' service - a red line offence resulting in immediate dismissal.

But it's not only about pay. That may reduce the instances of petty crime, and may make it harder for a terrorist organisation to exploit a member of staff, but where a terrorist wishes to gain a job at an airport, the salary offered will be the last thing on their mind.

It only takes one person to cause a disaster and given the size of many airports around the world, with tens of thousands of employees, many of whom are low-paid, transient workers, identifying 'bad eggs' is no easy task, especially in an environment which is driven by speed, customer service and on-time performance.

Whilst we all want 100% security, that is an impossibility. One only has to look to the tragic events of 5th November 2009 at Fort Hood in the US, when Major Nadal Malik Hasan, a psychologist in the US military, killed 13 fellow service personnel and injured 30 others. Or, 16th September 2013 when Aaron Alexis, a civil contractor to the US Navy, killed 12 and injured three others in a shooting at the Navy Yard in Washington DC. If we can't identify the insider threat in a military environment, where everybody goes through intense screening, how can we do so in airports?

The insider threat to aviation is actually not new. On 11th April 1955, an Air India flight was destroyed by a bomb infiltrated on board by a cleaner at Hong Kong International Airport, with the aim of assassinating Chinese Premier Zhou Enlai who was supposed to be – but wasn't - on board. The aircraft crashed into the sea near the Natuna Islands killing all on board. But that's history…

In the 21st century there have been a disturbing number of plots identified involving insiders.

In 2007, Russell Defreitas and Abdul Kadir conspired to blow up fuel tanks, and a fuel pipe line running beneath New York's JFK airport. Defreitas, the plot's originator, was a cargo employee at JFK and had been carrying out a surveillance operation, videoing facilities and then taking footage to Guyana where Kadir, who had connections with militant groups in Iran and Venezuela, was based and where the plot was being developed.

In 2009, Rajib Karim, a software engineer working at British Airways' call centre in Newcastle, UK, started to be in direct contact with Anwar al-Awlaki (key player in al-Qaeda) himself and was discussing how to use his position to perform a cyberattack against his employer. Karim was also exploring ways of achieving his ultimate goal of becoming a suicide bomber and was discussing with al-Awlaki whether he should become a member of cabin crew during a strike by BA's flight attendants.

And then, in 2013, Terry Lee Loewen, a technician with Hawker Beechcraft, was arrested at Wichita Mid-Continent Airport when he was trying to infiltrate a van laden with what he believed were explosives. In actual fact, the explosives were inert and had been given to him by the FBI in a sting operation. Loewen became a person of interest when he became a Facebook friend of somebody expressing jihadi sentiments; an FBI agent then befriended him and Loewen told him that he wanted to carry out an attack. Together they planned the mission and Loewen was arrested only when the authorities found him actually using his security clearance to enter the airport.

> "…arrested for having facilitated the transport of 153 guns on 20 different flights operating between Atlanta and New York…"

These three incidents actually demonstrate that, in the UK and US at least, the insider threat exists. However, they also show that effective surveillance operations can prevent plots from becoming reality. In the case of Loewen, whilst many might argue 'entrapment', the FBI's activities demonstrated the effectiveness of a red-teaming operation that ought to be replicated around the globe.

The monitoring of airport employees' social media transactions has now become an essential element of an effective aviation

The crew of flight KGL9268 are remembered at Kogalymavia's offices in Russia (Credit: Yuri Kochetkov)

Islamic State's online magazine, Dabiq, published a photograph of what it claims to be the IED which nrought down Metrojet flight KGL9268

security regime. Whilst this may appear to be an invasion of privacy, the stakes are so high that our not doing so may result in future atrocities failing to be prevented.

Last month, my own Lead Editorial for this journal addressed the value of Facebook surveillance of the pilot community:

"Whilst it was unfortunate that a March 2015 Australian Federal Police (AFP) report, marked 'For Official Use Only' was leaked to the press, its contents should serve as a reminder that some of the world's most ruthless organisations are determined to infiltrate the ranks of our pilots, and have already succeeded in doing so. The report stated that, "On 16 March 2015, information was received by the AFP that indicated two possible Indonesian pilots, likely employees of AirAsia and Premiair, had posted information on their Facebook pages that inferred support to the Islamic State."

Airside criminal activity is commonplace and hardly a week goes by without reports emerging of people with security clearance being arrested for their involvement in luggage theft, extortion, human trafficking, gun running, drug trafficking and facilitating the illegal movement of people across international borders. There are simply too many to list, but the following are a selection of some of the more significant incidents that have taken place in the last 12 months:

- September 2015: 25 employees of the Office of Transport Security in the Philippines were suspended in response to complaints from passengers departing Manila that they had been subject to extortion attempts.
- July 2015: The FBI indicted 46 people in a wide-ranging drug sting in the Dallas area; four of them were airline workers based at Dallas-Fort Worth International Airport.
- June 2015: Five members of staff at Entebbe Airport, Uganda, were arrested for their involvement in facilitating the smuggling of more than 600kgs of ivory onto a flight to Singapore. The shipment, which was labelled as videography equipment bypassed security checks as a result of bribes being paid (allegedly equivalent to a year's salary) by the smugglers.
- May 2015: In Vienna, Austria, a group of airport employees, including two employed in aviation security activities - one by G4S - were arrested for their involvement in smuggling illegal migrants to the UK.
- May 2015: In Venezuela, 24 criminal gangs were identified to be operating at Simon Bolivar International Airport, resulting in the arrest of 42 airport-based employees.
- February 2015: Two airport security screeners, contracted by the Transportation Security Administration at San Francisco International Airport, were arrested and charged with bribery and drug trafficking, having been found to accept money in order to allow quantities of methamphetamine through the passenger screening checkpoint.
- December 2014: Eugene Harvey, a Delta Air Lines employee, was arrested for having facilitated the transport of 153 guns on 20 different flights operating between Atlanta and New York.

How is it possible that somebody could get guns airside on a regular basis in an airport in the supposedly post-9/11 ultra-secure aviation environment? In the United States, the answer is simple – airport employees, aside from at a handful of airports, do not undergo routine screening when they pass from landside to airside. If they have been authorised to hold a pass to a security restricted zone, then they can come and go as they please. True, there may be the occasional random inspection, but for the employee who knows the ropes and the routines this is a limited deterrent.

> "…where are the demands that the US implement screening for airside employees…"

And this is where politics comes into play. It must be exasperating for the Egyptian authorities who, in the aftermath of the Metrojet disaster, are being cast as the villains of the piece - providing inadequate screening, unable to control who comes and goes and incapable of maintaining international standards – that foreign governments, some of whom had nothing to do with the flight in question, were quick to send in investigators, hasty to demand new screening protocols and had no qualms about grounding flights. Where was the international action against US airport security after the aforementioned incidents in San Francisco and Atlanta? Where are the demands that the US implement screening for airside employees – an industry standard in nearly all parts of the developing and developed worlds? What limitations were placed on foreign operators after the TSA failed 95% of its penetration tests? Apparently we cannot mess with Uncle Sam!

I am not sure what needs to happen for the industry – and government – to start to demand an intelligent security regime. For now, we seem hell bent on pursuing more of the same – more screening, using technologies with inherent limitations, rather than educated screening, using better calibre employees. The best modern-day example of the limitation of technology lies with the printer toner cartridge plot of 2010, where the printer intercepted

"…the deployment of screening technologies is of fundamental importance as an effective way of screening for and/or resolving a host of security threats. But no single solution addresses them all…"

at the UK's East Midlands Airport was intercepted and subjected to screening by X-ray and explosive trace detection; it was also physically searched, but no bomb was found and the package was cleared for onward transport to the US. If we, in the UK, can't find a bomb using multiple technologies and physical inspection when we know that there might be a bomb in a specific bag (Saudi intelligence had actually provided us with the specific air waybill number), how can we ever expect to find one using the same approach for screening millions of bags and cargo consignments when there is no specific threat identified?

Let's be clear – the deployment of screening technologies is of fundamental importance as an effective way of screening for and/or resolving a host of security threats. But no single solution addresses them all; aircraft have been hijacked using items which are not prohibited and, indeed, with no weapon at all. However, when a person or item does cause concern, the first, and safest, way of effecting an inspection is by an automated solution. The very fact that terrorists have had to become increasingly ingenious about the way in which they do infiltrate weapons and explosives onto aircraft (and, as a result, less successful as we saw with the likes of Reid and Abdulmutallab) is because of the significant developments in the screening technology arena, rendering traditional concealments foolhardy. And we should not ignore the deterrent value, which is why, regardless of detection capability, the failure to screen airport staff in the US is such a concern.

Twice now, Halloween has proven to be a nightmare for the Egyptian authorities. It was on 31st October 1999 that an Egyptair pilot, Gameel al-Batouti, is believed to have crashed his aircraft whilst it was en route from New York to Cairo, killing all 217 people on board. 16 years later to the day, 224 people were to die on the Metrojet flight leaving Egypt for Russia. Both incidents, it would seem at this stage, exemplify the insider threat…and, in these cases, Halloween was not celebrated in the spirit one would wish. Small wonder the insider threat is the subject which 'keeps airport security managers awake at night' - it's seriously scary!

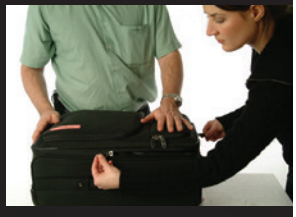
Philip Baum is Editor, Aviation Security International and Managing Director, Green Light Ltd. He is also the author of the book, 'Violence in the Skies: a history of aircraft hijacking and bombing, which is to be published by Summersdale in March 2016 and is already available for pre-order from Amazon. He can be contacted at: editor@avsec.com

GREEN LIGHT

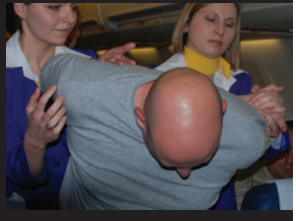
AVIATION SECURITY
TRAINING & CONSULTANCY

- DISRUPTIVE PASSENGER RESTRAINT
- INFLIGHT SECURITY
- HIJACK EXERCISES
- BAGGAGE & BODY SEARCH TECHNIQUES
- BEHAVIOURAL ANALYSIS
- QUESTIONING TECHNIQUES
- AVIATION SECURITY CONSULTANCY

RESPONDING TO THE THREATS...



...OF AN EVER CHANGING WORLD



WWW.AVSEC.COM