Picture credit: Getty

INSIDER THREAT

Mark Brace *examines the importance of dealing with the potential security threat posed by disgruntled airport employees*

As airports start to get back to normality after lockdown, it is vital that corners are not cut

Unless your airport is located in an active conflict zone, when we discuss threats, typically we think of terrorists or other extremist/violent non-state actor (VNSA) groups. There are a multitude of methods that such hostile entities could employ, including bladed weapons, a marauding firearms attack, improvised explosive devices, hoaxes and cyber attacks, as well as a range of potential targets – passengers, staff, security, facilities and aircraft. However, there is one thing that could make all of these more likely to succeed – an insider.

A well-placed insider can render even the most advanced technology or well-trained workforce ineffective, and will almost certainly guarantee at least some level of success in less secure and more corrupt locations. Insider access at an international airport was a crucial factor in two of the most recent 'successful' terrorist attacks against aircraft. In October 2015 at Sharm el-Sheikh Airport in Egypt, an insider is believed to have facilitated an IED concealed in a drinks can onto a Russian airliner; this detonated over North Sinai, downing the aircraft and killing all 224 on board. In February 2016, a senior security figure at Mogadishu Airport helped move an IED concealed in a laptop computer through security; this was subsequently detonated on board a Daallo Airlines flight to Djibouti by a suicide operative, killing only himself. The aircraft landed safely despite a gaping hole in the fuselage.

While these attacks involved insiders in ideal positions to facilitate airport attacks, they targeted aircraft. What about the threat to airports themselves? Of two major terrorist attacks against airports in 2016, in Brussels and Istanbul, there was no apparent insider assistance. Both targeted the relatively freely accessible landside areas, not requiring any kind of privileged access. However, it later emerged that one of the Brussels attackers had worked at the airport, albeit a number of years previously. Given the nature of the attack – the bombers detonated IEDs concealed in suitcases while inside the terminal building – there was no requirement for specialist insider expertise, although even basic historical knowledge could have assisted. In this case, however, there was no indication that he had been radicalised at the time he was employed. Therefore, any measures in place to counter such activity during his employment are unlikely to have had any impact on what eventually transpired.

It is important to know your staff to be able to spot any early or obvious signs of potential vulnerability. There have been numerous examples in recent years of airport workers coming to the attention of authorities due to suspected or proven extremist beliefs. In 2017, an investigative journalist alleged that four employees at Montreal Trudeau Airport had viewed extremist material online. Two were reassigned and two reportedly had security accesses removed as authorities were concerned over their mental well-being. The airport stated that it had robust procedures and checks in place, including ongoing vetting, to deal with such cases. There was no indication of any threat to the airport or those using it and it is unclear how the activity was discovered.

DISGRUNTLED EMPLOYEES CAN BECOME A THREAT AS AN EXTREME RESPONSE TO LABOUR DISPUTES

It is also crucial to work effectively with security and intelligence agencies, as insiders may be particularly effective in hiding their intentions. In 2015, avionics technician Terry Loewen pleaded guilty to attempting to explode a car bomb at his place of work, Wichita Dwight D Eisenhower National Airport in Kansas, USA. In December 2013, he had attempted to use his privileged access to drive onto the tarmac in what he thought was an explosives-laden car to carry out a suicide attack. Unbeknownst to Loewen – a radicalised Muslim convert – he was in contact with an undercover FBI agent, and the explosives in the car were inert. Everyone who knew him was unsuspecting; he had come to the attention of the FBI through his use of online forums. In October 2017, a Biman Bangladesh Airlines pilot was among a number of individuals arrested allegedly in the planning stages of an attack involving the hijack of a civilian aircraft. The precise nature of the plot and the pilot's involvement was unclear; however, he would theoretically have been in the ideal position to carry out such an attack.

Not all insiders are knowing participants in hostile activity; however, educating staff on the importance of protecting sensitive information is a key part of fostering an effective security culture. In May 2019, a New York court convicted Lebanese-born, naturalised US citizen Ali Kourani on multiple counts including terrorism-related charges. Kourani had been accused of being an overseas 'sleeper' operative for the Lebanese Hezbollah VNSA group, for whom he was carrying out procurement and attack-planning support activity. Evidence showed he gathered extensive information on New York JFK and Toronto Pearson airports, including details of security procedures, equipment and facilities, and questions asked by screeners. Kourani obtained some of this information through forging relationships with airport employees, who divulged security details – sometimes unwittingly, sometimes knowing of Kourani's provenance. US prosecutors assessed this information would have been used to facilitate people, weapons and contraband through the airports; however, it could also have been of use to operatives seeking to carry out attacks.

A different kind of insider threat has been highlighted by incidents involving employees commandeering aircraft without permission. Such cases often end in the perpetrator deliberately crashing the aircraft; subsequent investigations frequently highlight mental health problems. This was tragically demonstrated by the 2015 Germanwings Airbus A320 crash in France caused by the co-pilot, who had previously been treated for suicidal tendencies and declared medically unfit to work. In August 2018, a ground service agent 'stole' an airliner from Seattle-Tacoma International Airport before crashing it in an uninhabited area; he was reportedly suffering from mental health issues. In March 2019 a South African pilot allegedly took an aircraft without permission from Gaborone's Sir Seretse Khama International Airport in Botswana, before flying to Matsieng Aerodrome 30km away, where he crashed it deliberately into the control tower and flying club, killing himself. This reportedly followed a domestic dispute at a function at the flying club. These incidents serve as a reminder of the importance of staff well-being, and particularly mental health.

Disgruntled employees can become an insider threat as a more extreme response to labour disputes or financial hardship. In March 2020, an American Airlines mechanic at Miami International Airport was sentenced to three years' jail for sabotaging one of the airline's aircraft in July 2019 in an apparent bid to obtain more overtime work. He was reportedly upset and suffering financially due to stalled contract negotiations between the airline and unions, a dispute which had been ongoing for over three years. The perpetrator was a naturalised US citizen from Iraq who had worked as an airline mechanic for over 30 years. While allegations arose in September 2019 that he had familial links to the extremist Islamic State group, no evidence was found of this.

Insiders might also be well placed to disrupt the IT networks and computer systems on which airports and airlines are so reliant. In 2011, British Airways software engineer Rajib Karim was jailed for 30 years in the UK for plotting to use his access to assist al-Qaeda in the Arabian Peninsula (AQAP), although he never managed to advance any actual attack plans. Increased digitisation and integration of systems gives rise to potential vulnerabilities, and cybersecurity should be at the forefront of any new technology being introduced, whether it is an airport website, air traffic control systems or GPS equipment. In April 2020, the Netherlands Court of Audit published a report stating that the cybersecurity of border control systems at Amsterdam's Schiphol Airport was insufficient and not future-proof. While completing the assessments, an insider threat test breach was undertaken; this uncovered 11 vulnerabilities within the systems, which have since been addressed.

These incidents provide examples of how insider threats can manifest themselves, with some suggestions on how to tackle the problem. But how do operators address the issue in a more strategic fashion? The International Civil Aviation Organization (ICAO) provides an appropriate framework with its Global Aviation Security Plan (GASeP), which seeks to

▶

"enhance the effectiveness of global aviation security". As the UN's aviation body, ICAO created the plan in response to UN Security Council Resolution 2309 – "Threats to international peace and security caused by terrorist acts: Aviation security" – which was the first such resolution focusing on terrorist threats to aviation, and followed a series of attacks that rocked the aviation industry in 2015 and 2016. Launched in 2017, GASeP offers five priority outcomes intended to expedite progress towards enhancing global aviation security that could form the basis of a plan to tackle the insider threat.

The first is to enhance risk awareness and response – understanding and assessing risk to identify gaps and vulnerabilities can effectively focus resources where they are needed.

Secondly, develop security culture and human capability. Fostering an effective security culture that cascades through all parts of an organisation, complemented with appropriate training, is essential. This ensures that a security-focused mindset becomes second nature to properly motivated staff.

Third, improve technological resources and foster innovation. Implementing cutting-edge solutions to support appropriately resourced staff can enhance security without impacting operational efficiency – perhaps even improving it.

Fourthly, improve oversight and quality assurance. To achieve sustained improvements to security, oversight and quality assurance should be continually monitored through effective processes, such as a Security Management System (SeMS).

Finally, increase cooperation and support. The pooling of information and experience is essential to improve security; unfortunately, sharing what might be considered by some to be commercially sensitive information is anathema to running a successful business, and similar blockages occur at state level with confidential intelligence. To surmount this, collaboration within and between industry entities and national bodies must increase to achieve at least a base level of understanding for all.

RECOVERY POSITION

At the time of writing, the aviation industry is facing an uncertain future as it attempts to recover from the collapse in demand for air travel due to the global COVID-19 pandemic. What does this mean for the insider threat and aviation security? It seems inevitable that the focus for airport security will be on readying facilities to enable the swift and safe resumption of operations. This is likely to manifest itself in a focus on biosecurity measures, health screening and sanitisation, as well as an acceleration of efforts to find security solutions that minimise human-human contact at airports. Amid the post-COVID-19 changes, airports and airlines must also cope with layoffs and a furloughed work force, factors that could breed discontent and push some individuals towards malicious intent; extremist groups might also seek to capitalise on this. At the same time, it could mean fewer staff being available to effectively implement and maintain security processes, including those intended to address the insider threat. As the recovery proceeds it is imperative that corners are not cut and that vigilance and effective security is maintained. As ICAO says in the GASeP: "Security is a critical pillar for the growth and sustainability of the global aviation industry". Right now, 'growth' means a return to pre-COVID-19 levels of activity, and the industry can ill afford any further major blows such as a terrorist attack as it follows this path ●

Mark Brace – Senior Aviation Security Analyst at Osprey Flight Solutions – has many years' experience as a senior threat analyst for the UK Government, with specific expertise in threats to aviation.

Insider knowledge gives the attacker a vital advantage

Picture credit: Getty