Turbulence ahead:

An overview of the enduring and evolving threat to civil aviation

Andy Blackwell, former Head of Security with Virgin Atlantic and now a Registered Independent Security Consultant specialising in Transport Security, provides insights into the enduring and evolving threats to civil aviation based on analysis of events during the first six months of 2017.

Threat landscape

AQ continues to demonstrate its desire to attack aviation and Ibrahim al-Asiri, AQAP's chief bomb-maker, is believed to be active in Yemen. The self-proclaimed Islamic State (IS) is also said to be evolving its capability to conceal improvised explosive devices in electronics, with several reports making specific reference to the group's research into the concealment of explosives in batteries and the battery compartments of electronics.

AQ, IS and their affiliates have the capability to attack civil aviation. Two poignant reminders of this are the Russian Metrojet bombing in Egypt, claimed by ISIL's Sinai Branch who said they used an IED concealed in a soft-drink can, and the Dallo aircraft bombing in Somalia, claimed by al-Shabaab, where airport insiders bypassed security controls and enabled a laptop bomb to be taken on board the aircraft.

Ironically, IS recently boasted about its cost-efficient destructive capability against aviation. For the second time, they released the image of the improvised explosive device they claimed downed the Russian aircraft over Sinai. Commentary accompanying the image mocked that the Massive Ordnance Air Blast (MOAB) bomb, which the U.S. used to target IS caves in Afghanistan and was said to cost millions of dollars, did not kill any IS operatives. However, their small fizzy drink can converted into an explosive at a negligible cost managed to blow up a Russian aircraft, killing hundreds.

The words of Homeland Security Secretary John F. Kelly help us understand the magnitude of the threat we're facing. Kelly recently stated that the heightened threat of terrorists taking down a commercial airline is one of his greatest concerns. He was quoted as saying, "*A thing that keeps me up at night is the intent of terrorists to knock an airplane down in flight*". *Jean-Paul Laborde, **Head of the UN Counter Terrorism Executive** Directive has warned that "it's a question of when, **not if**"* terrorists use laptops to smuggle bombs onto aircraft. The UN Secretary General has also reported that there continues to be a serious and enduring threat from international terrorism to our transport networks – specifically to civil aviation.

Peter Neffenger, the former Head of TSA, warns that terrorists are competing for supremacy in aviation terror attacks. "*Whether it's ISIS, AQAP, or other up-and-coming terror groups, they all have master bomb-makers and access to extensive knowledge bases that make the terrorist threat to airplanes – specifically those flying to the U.S. – **more dangerous than ever***". He added that there are more potential threats out there than ever before.

Knowledge transfer risks and a potential increase in the number of actors with the capability to attack the industry is likely to be fuelling concerns about the evolving nature of the threat.

The U.S. and UK authorities, in response to the evolving threat, implemented additional security measures from specific last points of departure to flights destined for the U.S. and UK. The UK restrictions ban phones, laptops and tablets larger than 16.0cm x 9.3cm x 1.5cm from being taken into the cabin on flights to the UK from Turkey, Lebanon, Egypt, Saudi Arabia, Jordan and Tunisia. Similar requirements in the U.S. also include flights to their jurisdiction from four additional countries; the United Arab Emirates, Qatar, Kuwait and Morocco. The decision is based on assessment of the threat environment in the respective countries and clearly there are differences of opinion between the U.S. and UK, which could also be linked to differing risk tolerances. U.S. security officials have demonstrated good risk-based selection and have lifted the ban where they have visibly verified that additional security measures have been implemented by airlines flying to the U.S.

The U.S. Homeland Security Secretary has made it clear that if intelligence showed any other threats he would not hesitate to expand the limitation on aircraft bound to the U.S. from other countries in addition to those already subject to the large electronics ban. A few weeks after the original ban, the DHS issued a Fact Sheet entitled Aviation Enhanced Security Measures for All Commercial Flights to the U.S., as Kelly has determined it necessary to implement enhanced security measures for all commercial flights to the United States following what he describes as a 'spider web' of threats to commercial aviation as terrorists pursue new attack methods. The U.S. assessment is based on evaluated intelligence. The measures, both seen and unseen, will include enhanced screening of passengers and electronic devices as well as heightened security standards for aircraft and airports.

Shortly after the initial security enhancements were announced, AQAP's Inspire magazine issue 13, was recirculated via one of their established media channels. The issue deals almost entirely with the targeting of commercial aviation. As publicly reported, the magazine gave details of the best place to detonate explosives whilst on an aircraft together with instructions for assembling improvised explosive devices and evading airport and airline security. The promulgation of such material unhelpfully spreads knowledge to those who may have sinister intent, whilst also creating a climate of fear.

ABOVE: The aviation sector faces increasing vulnerability to cyber-attacks as technologies and connectivity becomes more widespread

ISIS – in their propaganda magazine Rumiyah – have also referred to a new tactic, arson, claiming how destructive operations of such simplicity can be. Whilst they have not specifically mentioned aircraft, fires in the aviation environment can and have had catastrophic consequences and it's important to consider this modus operandi when risks are being assessed.

It's not just physical attacks that the industry must concern itself with, however. The aviation sector also faces increasing vulnerability to cyber-attacks as technologies and connectivity with the Internet of Things becomes more widespread. Of particular concern is the increasing risk to cyber security and its resulting threats to the integrity of data and critical operating systems.

Threats and risks: Initial findings

Evaluation of reporting for the period of 1 January 2017 to 30 June 2017 reveals the following:

- The terrorist threat to civil aviation is enduring and evolving
- Knowledge transfer (of IED construction and terrorist modus operandi) is a cause for concern, as the number of threat actors targeting the industry may increase if this occurs
- There is an increased risk to the industry's information systems as technologies and connectivity develop and attacks against other sectors proliferate, with cybersecurity needing to play catch up
- Several of the incidents involved individuals suffering from mental health issues, rather than terrorism, but none-the-less threaten security
- Key aviation stakeholders and their representative bodies believe that information sharing between governments and industry is key to staying one step ahead of emerging threats
- Many incident response actions are taken out of an abundance of caution, despite a lack of threat credibility
- The complexity of some security requirements impacts compliance
- There is an inconsistent approach to gauging security assurance.

Despite the enduring terrorist threat we should never lose sight of all the good work being done to help keep the industry safe and secure. These are some of the highlights:

The UN Security Committee adopted Resolution 2341(2017) on protection of critical infrastructure, including airports and other transport systems, against terrorist attacks. The resolution calls on states to improve preparedness; and it strengthens cooperation in protecting the security of our people and our critical infrastructure.

ICAO's inaugural Cyber Summit convened by ICAO called for every nation to address the risk that cyber terrorism poses to its civil aviation industry; to build their own capability to address such threats and ensure that the laws that govern such criminal activity are fit for purpose.

EASA, the European Aviation Safety Agency, has signed a Memorandum of Cooperation with the Computer Emergency Response Team (CERT-EU) of the European Union institutions, to protect against intentional and malicious cyber-attacks. EASA and CERT-EU will cooperate in the establishment of a European Centre for Cyber Security in Aviation (ECCSA), to provide information and assistance to European aviation manufacturers, airlines, maintenance organisations, and air navigation service providers.

IATA is playing an important co-ordinating role bringing together key stakeholders including airlines, air navigation service providers and aircraft manufacturers to develop a common cybersecurity framework. Muhammad Ali Albakri, IATA's Regional VP for Africa and the Middle East, reports that the global aviation industry is increasingly focusing on cybersecurity, which has become a major concern that the industry is still "*trying to get to grips with*". *IATA has adopted a resolution reaffirming the industry's commitment* ***to safety and security. It also made a call for*** *greater collaboration between government and key industry stakeholders. Alexandre de Juniac, Director General and CEO, said: "Information sharing among governments and with the industry is key to* ***staying a step ahead of emerging threats***".

The TSA promoted its new national framework designed to improve security around public spaces at airports, particularly those areas located outside of security screening. The recommendations for local governments and transportation systems are a direct response to growing concerns over

ABOVE: There has been tight U.S and UK restrictions on large electronic devices being taken on some flights

'soft targets' following the 2016 mass fatality airport attacks in Brussels and Istanbul, which highlighted the evolving tactics and techniques that adversaries use to attack civilian targets in public areas. This is an excellent example of the collaborative approach, with representatives from industry, government and academia working together to evaluate security measure gaps in the current system and come up with ideas to enhance security.

The UK CAA continues to build on the work of their Department for Transport (DfT) colleagues and support industry as interest in Security Management Systems (SeMS) grows. CPNI project work researching SeMS across the critical national infrastructure and linked organisations is providing valuable insights too. The UK DfT is updating and enhancing their Industry Threat Assessment training package and delivery methods in partnership with aviation representatives and external specialists.

Conclusions

The aviation sector is facing challenging times due to the enduring and evolving threat from international terrorism. Terrorists remain committed to targeting the industry and the transfer of knowledge between groups may increase the number of hostile actors and frequency of incidents we face in the future.

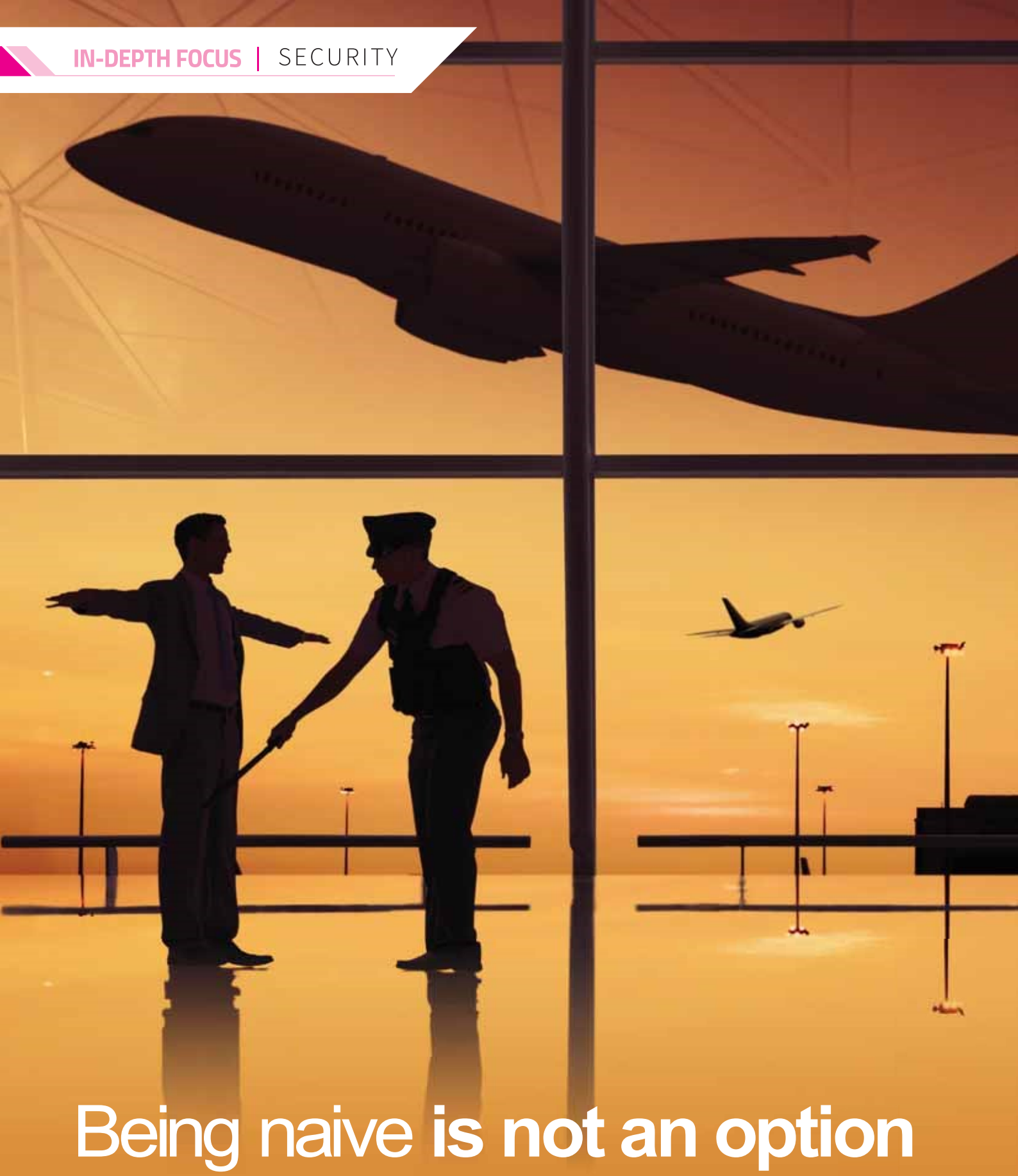
Furthermore, incidents arising from mental health issues are less predictable than many terrorist threats – potentially making them harder to predict and protect against.

Positive security outcomes are best achieved through partnership approaches and recent examples of this include the TSA's Soft Target work, the UK CAA's ongoing Aviation SeMS work, CPNI's SeMS Research Project, DfT's Industry Threat Assessment training refresh, EASA's work with CERT-EU developing a European Centre for Cyber Security in Aviation, IATA's call for a more collaborative approach on security between governments and key industry stakeholders and their ongoing work developing a common cybersecurity framework. Collaborative approaches will help government and industry achieve common goals.

Adopting a SeMS approach will help industry move away from the '*terrorists act then we react'* cycle, to deliver more confident and informed security, threat and risk management. A robust SeMS will produce assurance beyond compliance under a simple framework that makes best use of an organisation's resources, policies, systems and tools. In this way, the industry escapes from an *'out of an abundance of caution'* mindset and the inefficiencies and costs that they cause.

BIOGRAPHY

ANDY BLACKWELL is former Head of Security at Virgin Atlantic and now Director of Blackwell Security Consulting, which specialises in SeMS development. Andy has been commended by the Metropolitan Police for demonstrating a high degree of professionalism and providing an exceptional level of service during a period of heightened threat against civil aviation.



Being naive is not an option

As the civil aviation industry continues to deal with the threat of terrorist attacks, *Roni Tidhar*, Head of International Consulting – Security and Safety, Ben-Gurion Airport, Commerce and Business Development Division, Israel Airports Authority (IAA), explores some key factors that every airport director or manager must address and preferably take further action on.