Journal of AIRPORT MANAGEMENT

SPRING 2018 VOLUME 12 NUMBER 2

ISSN 1750-1938

An International Journal

ACI AIRPORTS COUNCIL INTERNATIONAL

Published in association with Airports Council International

HENRY STEWART PUBLICATIONS

Airport security threats and strategic options for mitigation

David Menzel

Jennifer Hesterman

DAVID MENZEL

is based at SITA's US offices in Atlanta, GA and has led sales as the Director, Government Markets since 2012. He has more than 25 years' experience in aviation and telecommunications leading sales, marketing and business development strategies for start-up, Fortune 500, venture capital-owned, foreign-based and privately-owned firms and organisations. David is responsible for coordination on strategy engagement for SITA's industry and legislative efforts on Capitol Hill. David organised and founded the Secure Journeys Working Group, which is a collaborative effort among airport stakeholders on utilisation of existing and innovative new technologies to ensure a secure journey for travellers. Prior to joining SITA, he enjoyed many years' extensive specialist experience in a range of airport solutions and systems integration, both within and outside the USA.

JENNIFER HESTERMAN

is a retired US Air Force colonel who served three Pentagon tours and commanded in the field. Her last assignment was Vice Commander at Andrews Air Force Base, Maryland, where she led installation security, force support and the 1st Helicopter Squadron, and regularly escorted the President and other heads of state on the ramp. She is Vice President, Business Resiliency and Education Services for Watermark Risk Management International, on the board of directors for the International Foundation for Protection Officers and advises the Homeland Security Training Institute at the College of DuPage. She holds a doctoral degree from Benedictine University, master of science degrees from Johns Hopkins University and Air University, and a bachelor of science from Penn State University. She was a National Defense Fellow at the Center for Strategic and International Studies in Washington, DC and is an alumnus of the Harvard Senior Executive Fellows programme. Her book, *Soft Target Hardening: Protecting People from Attack*, was the ASIS Security Book of the Year for 2015. She also authored *Soft Target Crisis Management* (2016) and *The Terrorist-Criminal Nexus* (2013). Dr Hesterman is an expert on international and domestic terrorist organisations, transnational threats and organised crime. She is one of the very few analysts specialising in the terror–crime nexus. She is also a consultant on soft target vulnerabilities and hardening tactics, and has a specialist interest in issues including human intuition, concentric rings of security and 'fifth column' insider threats.

Abstract

This paper provides an overview of the security challenges and responses faced by airports. The number of air passengers is doubling every 15 years just as security dangers multiply across the world. Technology is enabling massive advances in security, but there are other elements that should be embraced — from exploring the power of human intuition to the lessons learnt by the military through the adoption of concentric rings of security and the very real dangers from insider threats. Cybersecurity is also an increasing and potentially catastrophic risk which, along with other emerging threats, needs to be addressed with greater creativity and imagination. Much is being done to deal with the risk — not least with industry programmes such as Fast Travel, Smart Security and now the International Air Transport Association's (IATA) and Airports Council International's (ACI) latest initiative, NEXTT (New Experience in Travel and Technologies) — but the message from every key organisation is that the industry must do more, particularly when it comes to political will and a readiness to share experiences and best practice.

Keywords

collaboration, soft targets, insider threats, cybersecurity, new technologies, intuition, secure journeys

David S. Menzel,
Sales Director — Government Markets, SITA,
3100 Cumberland Blvd,
Suite 900,
Atlanta, GA 30339,
USA

Tel: +1 770 548 0682
E-mail: david.menzel@sita.aero

Jennifer Hesterman,
Watermark Risk Management International, LLC,
4023 Maple Ave Suite 100,
Fairfax, VA 22032,
USA

Tel: +1 703 621 0045
E-mail: jennihesterman@gmail.com

FACING THE ISSUES

Air transport has had to respond to the threat of terrorists for more than 40 years, as they constantly seek to exploit the industry's vulnerabilities. Airports need to be able to deliver a convincing, pervasive but also cost-efficient and empathetic security infrastructure — capable of

handling not only travellers and those seeing them off/welcoming them, but also the tens of thousands of people needed to provide airport services on a day-to-day basis. This security infrastructure must also be in line with international obligations, set out in UN and International Civil Aviation Organization (ICAO) standards.[1]

Physical security is crucial, but — thanks to its interconnectivity, complexity and weight in the economy — cybersecurity has also become an attractive target.

SITA research suggests very high levels of security awareness among staff at airports (85 per cent) and airlines (82 per cent). Already, chief information officers (CIOs) at 47 per cent of airports and 69 per cent of airlines are implementing security events and correlation monitoring, while security incident response management is being put in place at 60 per cent of airports and 77 per cent of airlines.[2]

Nevertheless, an increasingly complex and high stakes security environment must also be seamlessly integrated with the need to optimise efficiencies of use of space and movement of people, given the tremendous growth in the number of passengers being experienced worldwide — rising from a forecast 4bn this year to 7.8bn by 2036, according to the International Air Transport Association's (IATA) latest indicators.[3] In their Global Market Forecast 2017–2036, Airbus notes a record 60 per cent market growth (measured in revenue passenger kilometres, RPK) in the last 10 years, 110 per cent since 9/11 — and they anticipate a similar doubling every 15 years at least through to 2036. This drives demand for new aircraft to fly more people. Airbus forecast demand for 34,900 by 2036, with 60 per cent of that — almost 21,000 aircraft — required for growth.[4]

As a result, airports can face the challenge of improving security within existing budget and facility constraints, requiring smarter solutions, as they become more congested with people and aircraft. This is a problem that cannot be solved by new infrastructure alone. Because of their complexity, airports require significant planning, take a long time to develop and build — the average airport master plan has a 20–30 year horizon — and they are massively costly. Larger airports capable of handling increased passenger numbers also require an enhanced supporting road/rail infrastructure.

FINDING THE RIGHT BALANCE

There are other factors hindering a watertight air transport security infrastructure. For example, regional airports have a difficult balancing act to fulfill. Australia-based Regional Express Airlines (Rex) made the point in August 2017 in a public statement relating to screening of passengers. They noted that 'smaller regional aircraft carry fewer passengers than most buses and it would be senseless to enforce screening on the former while leaving "vulnerable" the tens of thousands of buses plying the streets each day.'[5]

The airline noted that they serve 45 regional communities, where screening was not required. They estimated the cost of screening would be AUS$34m a year in extra costs, when their operational profits for FY 2016 were just AUS$4m. If screening was mandatory, they noted, the result would be that most regional centres would be left without an air service, with a devastating impact on regional communities that depend on air services.

Nor is the issue of balancing security needs against the practical realities of operating regional airports limited to the particular geography of Australia.

Airports Council International (ACI) World released a Policy Brief on Airport Networks and Small Airport Sustainability in February 2017, in which they estimate that 66 per cent of the world's airports operate at a net loss. As many as 92 per cent of those losing money handle fewer than one million passengers a year.[6] A large proportion of the 450+ commercial airports in the USA handle less than one million passengers — and they will continue to face mounting pressure and associated costs related to security and evolving threats.

With space at almost every airport at a premium — and with more passengers arriving for and leaving from more planes — more space might be considered essential for requisite security. But, focused on reducing their losses, airports are increasingly dependent on retail and other non-aeronautical revenues to balance the books. It means that precious space must be made to work harder, without compromising an effective security strategy. With disruptive technologies and businesses such as Uber and Lyft affecting parking revenues, the pressures will continue to challenge the entirety of the system.

PATIENT TO IMPATIENT

It is a long-held ambition of the industry to get passengers efficiently and effectively from curb to gate in order to mitigate/remove passenger pain points. This is reinforced by the visions of industry programmes such as Secure Travel and the latest IATA/ACI New Experience in Travel and Technologies (NEXTT) initiative,[7] announced in October 2017.

Certainly passengers would appear to have had enough. The length of time they consider as acceptable to be queuing at security checkpoints has changed markedly. In 2012, 21 per cent were prepared to queue for 10–20 minutes, 51 per cent thought between 5 and 10 minutes was acceptable, while just 27 per cent expected a wait of 5 minutes or less. By 2015, 7 per cent were prepared to queue for 10–20 minutes; a broadly similar 48 per cent found a wait of between 5 and 10 minutes acceptable, while those expecting a wait of 5 minutes or less had nearly doubled to 45 per cent.[8]

The importance of moving passengers swiftly into a more secure environment post-security is now recognised by a growing number of government agencies — including customs, immigration and those responsible for regulating and controlling landside spaces for security purposes — just as for any other similar public space such as an intermodal metro/subway or railway stations. They also increasingly understand the criticality of working together.

For example, in September 2016, the first of a series of Transportation Security Administration (TSA)-sponsored public area security summits noted that:

> Instead of operating with competing authorities, funding streams, and areas of ownership, we sought to turn this approach on its head. Looking around the room we realized that we had all the authorities needed, multiple funding streams to take advantage of, and the world's leading experts. The only thing that was missing was a collaborative framework, leveraging those authorities and independent efforts.[9]

The summit produced a series of recommendations designed to enhance security at airports and across the transport system, under three headings: information sharing, attack prevention, and infrastructure and public protection.

The summit included relevant bodies not previously included in aviation or

other transport security plans and has established lines of communication between US and international airport managements.

BALANCING TECHNOLOGY WITH HUMAN INTUITION

Striking the right balance with security solutions is always a tricky issue to resolve. There can never be a completely safe environment, which is why all bodies emphasise the need for security solutions that are:

- Risk-based: proportionate to the threat and focused on the probable, not the possible.
- Outcome-based: achieving stated security objectives, rather than prescriptive and rigid procedures.
- Facilitation-based: that is, as far as possible not disproportionately disrupting people's lives.

The air transport industry is agreed on the need for increased coordination and collaboration between airlines, airports, regulators, law enforcement agencies and intelligence communities to effectively address the threat trajectory and quality of aviation security measures.[10]

In response, airports today are the focal point of security innovation. New technologies are providing airports with unprecedented levels of information and intelligence, thanks to the evolution of big data, mobile technology, artificial intelligence and machine learning.

Perhaps the area of greatest interest is in biometrics and identity management. Much of this work has been channelled through the IATA/ACI Smart Security programme, launched at the end of 2013[11] and designed to move aviation security to a model that will effectively facilitate faster processing for low risk travellers that have been reliably identified using their live biometric data. The model extends across the process of booking tickets, entering the airport, check-in, security screening, boarding and departing, getting to know real-time conditions and actions, trying to identify abnormal conditions in advance, taking the initiative to prevent risks, and conducting appropriate and targeted measures, so as to realise intelligent management and control during the whole process.

Smart Security concepts and solutions have been tested and evaluated in partnership with governments, airports, airlines and solution providers. Airports — including Geneva, London Heathrow, Amsterdam Schiphol, London Gatwick and Melbourne — were early pioneers, with many more now looking at how Smart Security concepts can be implemented.

SMART INTEGRATION

SITA's Smart Path™ is an approach to identity management that uses biometrics at every step in the passenger journey to identify travellers. It is easily integrated into existing airport infrastructure and dedicated airline systems, including standard common-use, self-service equipment already in use across the industry such as check-in kiosks, bag drop units, gates for secure access, boarding and automated border control, making deployment rapid, easy and cost-effective.

Smart Path™ also integrates with government systems and databases, allowing integrated immigration and border checks. Designed to be modular, it allows airports to implement whole journey identity management into passenger self-service touchpoints.

Not only does the use of biometrics speed up the whole airport process — it also enables security resources to be based on risk (the definition of which is also becoming ever more sophisticated thanks to technology) — allowing airport facilities to be optimised. This creates a virtuous circle with the enhancement of passenger service at its heart. For example, since the introduction of facial recognition technology at Shenzhen Airport, 701 persons who fraudulently used others' documents or used counterfeit documents were detained, and 158 persons wanted by the police were identified and captured.[12]

Civil aviation security in the future will go beyond identity management, making full use of the sensing technology of the internet of things to mobilise law enforcement resources, monitor the real-time conditions of passengers, staff, vehicles, cargo and luggage at the airport in an intelligent, efficient and precise way, identify potential risks, and make optimal deployment of security resources.

NEVER FORGET INTUITION

Technology is central to the provision of strong solutions capable of handling the need for effective security; however, military doctrine asserts that 'the human is the best weapon system'. Therefore, it is essential that society as a whole resists the tendency of an over-reliance on security technology marginalising the importance of human involvement. For example, US Customs continues to insist on face-to-face interviews, even in the case of passengers using self-service automated passport control (APC) kiosks that SITA developed and that provides for the input of all data required for immigration clearance.

It is increasingly clear that intuition is one of the most under-appreciated natural human gifts — the ability to know something from instinctive, rather than conscious, reasoning or proof of evidence.

Which is why the US military — notably the Marine Corps — has undertaken a substantial amount of work on intuition. This includes honing and trusting the sixth sense as the 'art' in the 'art and science of war' discussed in their teaching.

Based on stories from combat veterans returning from Afghanistan and Iraq about situations where intuition saves countless number of lives on the battlefield, the Office of Naval Research is studying how military members can hone their intuition. Their research in human pattern recognition and decision-making suggests there is indeed a 'sixth sense' through which humans can detect and act on unique patterns without consciously and intentionally analysing them.[13] And, unlike machines, they believe that humans are the best sensors.

USING CONCENTRIC RINGS OF SECURITY

The faster and more easily passengers can move through an airport's non-secure areas, the greater the security of the airport — and the greater the opportunities for them to enjoy the retail, food and beverage, and other resources put at their disposal as they wait for their flight.

In the USA, the TSA already employs the concept of layers of security, with 20 integrated components working together to protect passengers, airports and aircraft.[14] This could be further enhanced through lessons learnt from the protection of military assets, involving the use of concentric rings (or barriers) of security

to both physical infrastructure and IT assets across the airport. Six physical rings can be identified.

The ramp and its aircraft are the critical node, or asset, at the centre of the circle, protected by access control. Surrounding the asset are those with direct contact, such as engineers, ramp personnel, baggage handlers, cleaners, those who load the food and fuel onboard, and flight crew. Included in the centre ring are the control tower and its staff.

The second ring includes those in the secured area of the terminal — such as screened passengers, gate personnel, retail and restaurant staff, maintenance and cleaning crew. The third ring is the public space of the terminal prior to security — including check-in desks, shopping and restaurants, and baggage claim. Beyond that is the ring around the terminal itself, including public access roads, sky trains, parking structures and short-term parking lots. The fifth ring includes the perimeter fence, extended parking lots, rental car agencies, consolidated rental car centres and intermodal facilities such as subway and train stations. Finally, the sixth, or outer, ring encompasses highways leading to the airport, access roads, gas/petrol stations, hotels and other businesses in the surrounding 'aerotropolis' community. Social media may also be considered part of the outer ring, as a virtual 'community'.

The centre rings have barriers meant to detect, prevent, deter and mitigate an attack or security incident, whereas the outer rings may provide a crucial over-watch role, designed to identify possible danger. For instance, most recent terrorist attacks at soft targets include pre-operational surveillance. As surveillance is an art and science, many rudimentary actors lack the requisite skill set, thus are sloppy and easily detectable to a trained eye. Conducting a vulnerability assessment on each ring may uncover a fracture leading all the way from the outer ring to the aircraft. This gap may be lack of communication between dissimilar organisations or the 'gatekeeper' of each ring, or inconsistent or incongruent policies that prevent timely reporting of important data points.

Technology is once again playing a commanding role in ensuring the rings work together. Self-service systems are streamlining access to each successively higher security ring. The use of proximity-sensing, object detection and big data is improving passenger flow and dwell time, reducing bottlenecks at the barriers between rings that result in vulnerable crowds. Beacons are leading to greater personalisation of mobile services for passengers. Big data and artificial intelligence are also leading to new tools for effective disruption management, reinforcing progress made in smoothing the passenger journey through the airport. The internet of things is ensuring that airports will be able to keep track of not only physical assets, but also staff and even passengers.

It is also complemented by SITA's Day of Operations BI (business intelligence) — a cloud-based business intelligence portal to view critical data, monitor, measure and predict daily operational flow challenges etc. — and Airport Management — a suite of integrated software applications that enable control of all airport operations from a central point, facilitating common situational awareness.

INSIDER THREAT: A FIFTH COLUMN

A major airport has the equivalent number of people as a medium-sized town, working within a far smaller footprint.

From engineers to airline staff, retail to airport management, baggage handling to cleaning and grounds maintenance, they include full or part-time employees, contractors, consultants, agency and temporary staff as well as travelling air crew. Many instances of breaches of security — from cybersecurity to theft, to fraud through to terrorism — result from actions by those working within the airport ecosystem.

For example, PwC's Global State of Information Security® Survey 2018[15] notes that across all sectors, current employees remain the top source of security incidents at 30 per cent, followed by former employees at 26 per cent.

Certainly, as we harden airport security, a determined bad actor may seek to utilise an insider to gain access. An increasing number of organisations now recognise the presence of nefarious inside actors as their number one security threat. Insiders may never act violently, but they can enable those who wish to do harm. An insider can be a force multiplier to an attack, with intimate knowledge of facilities, operations and vulnerabilities. Using access, they can also pre-position supplies for themselves or others, and assess the perfect time to strike and obtain the maximum results, whether casualty counts, damage to the physical airport or even the organisation's reputation.

There is a persistent lack of research and data analysis regarding the insider threat, making it the least understood and least appreciated danger to an organisation or venue. Compounding the problem are organisational and cognitive biases leading managers to downplay the insider threat. Indicators used to detect threats with outsiders fall short, as do countermeasures. We inherently trust the insider — not least because they have a legitimate job and role in the work place. There is a tendency to assume disgruntled or troubled employees have outward signs of hostility at work. Although some workplace attacks occur by recently fired employees, many others come as a complete surprise. Risk assessments have not tended to include insider threats, but they must do so, in order to fully protect the organisation and its staff, the public and stakeholders.

Good hiring practices are the first line of defence, but the screening process itself has many flaws: deception experts believe that up to 50 per cent of applicants lie on their resumes and job applications, and 80 per cent lie during full screening interviews.[16] A thorough background check is essential, while pre-employment screening by experts using psychometric techniques is a good front line of defence for those working in secured areas of the airport.

NO DARK CORNERS

A great deal of time is spent screening and clearing employees during recruitment, but far less time is expended on day-to-day assurance that an employee is still reliable and fit to perform duties in sensitive areas. Everyone has their public life, private life and secret life — the latter of which may bring unforeseen danger to the workplace. The 'no dark corners approach' offered by author Nick Catrantzos illuminates these possible shadows in the workspace (Figure 1).[17] First, a cultural shift is needed: everyone is responsible for securing the workplace. Secondly, new employees might be hired on a probationary basis with a long-term, trusted employee as mentor. Thirdly, the physical workplace should be transparent; employees have the right to privacy, but an open work area should be constructed where the workspace is visible. When it

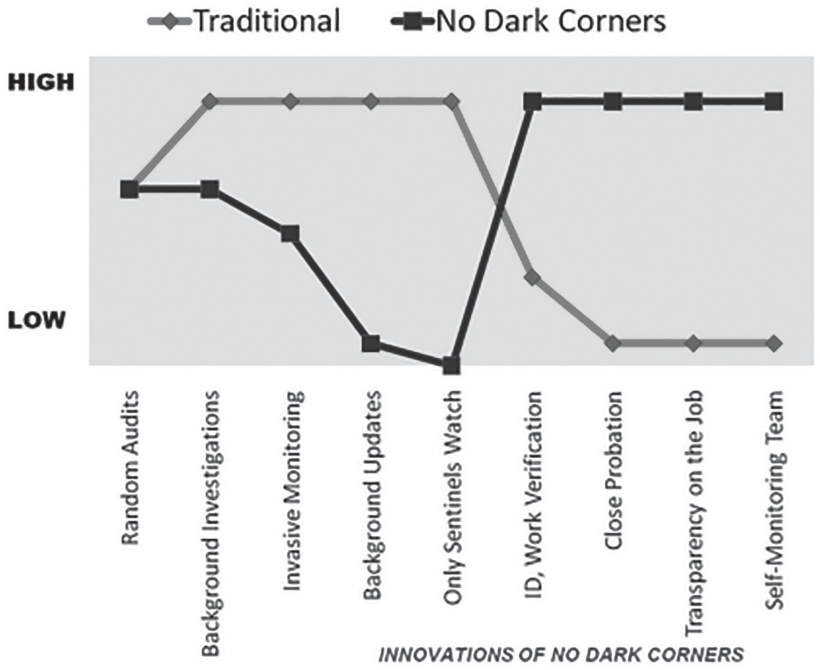

Figure 1 No dark corners
Source: Catrantzos, N. (2010) 'No dark corners: A different answer to insider threats', *Homeland Security Affairs Journal*, Vol. VI, No. 2, available at: https://www.hsaj.org/articles/83.

comes to the insider threat, there is truly safety in numbers.

Airports may take a few pointers from the nuclear security realm, in which a nefarious insider could lead to catastrophic results. Matthew Bunn and Scott Sagan authored an informative piece about worst practices and failures in the nuclear industry regarding the insider threat, with solutions that may be cross-applied to soft targets.[18] The authors encourage facility owners and security managers to identify and challenge assumptions, stating:

- Do not assume that serious insider threats are NIMO (not in my organisation).
- Do not assume that background checks will solve the insider problem.
- Do not assume that red flags will be read properly.
- Do not assume that insider conspiracies are impossible.
- Do not assume that organisational culture and employee disgruntlement do not matter.
- Do not forget that insiders may know about security measures and how to work around them.
- Do not assume that security rules are followed.
- Do not assume that only consciously malicious insider actions matter.
- Do not focus only on prevention and miss opportunities for mitigation.

Fighting these assumptions, use of psychometrics in the screening process and the 'no dark corners' approach — including the use of open sources such as social network presence, perpetual vetting against updated watch lists, etc. — can go a long way towards thwarting the insider threat in airports.

From a technology perspective, access security for airport staff has tended

to rely on a series of tried and tested procedures coupled with conventional token or PIN-based access controls. Biometric identification, however, ensures the identification is reliable, linking back to the vetting of the airport staff member that was conducted at the time of enrolment in the system, with subsequent updated assessments. Biometrics also enables access to secure areas on the basis that those responsible for security are able to identify who an individual *is*, as opposed to what they are carrying or what they know. Biometric identification can also be automated, removing a further potential point of weakness.

ADDRESSING CYBERSECURITY THREATS

In their report 'Strengthening digital society against cyber shocks', PwC quote the US National Intelligence Council's 2017 global trends report's caution that society faces the 'imminent' risk of cyber disruption — potentially with 'lethal consequences' — owing to the vulnerability of crucial infrastructure.[19] They add that many people worldwide — particularly in Japan, the USA, Germany, the UK and South Korea — are concerned about cyberattacks from other countries.

As the digital world has increased in reach and complexity, the attack vectors, threat actors and opportunities have multiplied. The increasing velocity and sophistication of threats are starting to take on decidedly vertical industry flavours, however, and the move towards digital business and ubiquitous connected devices continues to accelerate this trend.

Security can take many forms in any given context. For the purposes of this paper, cybersecurity includes the entire internal IT infrastructure view (including physical perimeter security), the hardware and software environments, the entire stack, information security, endpoints, and both offensive and defensive capabilities. As digital ecosystems grow, this cybersecurity view also grows into broad external linkages and the digital footprint of partners, creating new challenges in an open digital world. Defence-in-depth is also relevant — a similar concentric rings approach to that discussed above.

Bear in mind four points. First, there is a 'detection deficit' between attackers and defenders: the time taken to compromise a victim is still far shorter than the time taken to discover the attack.[20] Secondly, in 60 per cent of cases, the attackers are able to compromise an organisation within minutes. Thirdly, where the motive of an attack is known, more than two-thirds are going after a secondary victim. Fourthly, because of the complete interdependence of the air transport industry, cybersecurity is only as secure as the weakest link. For example, in January 2016, the head of Thales avionics business acknowledged a connection between the cockpit avionics system and the cabin in-flight entertainment system that cyber attackers could potentially exploit.[21]

ALL TOGETHER NOW

To address the issue successfully, the hows and whys of the attackers need to be fully understood. Intelligence is crucial, which is why the work being done as part of ICAO's Civil Aviation Cybersecurity Action Plan is so important — as is the creation of ACI's Cybersecurity Taskforce and the ACI IT Security Benchmark, based on ISO 27002, and IATA's Cybersecurity Toolkit.

As with all areas of security, everyone in the organisation must take responsibility for investing in the security of their part

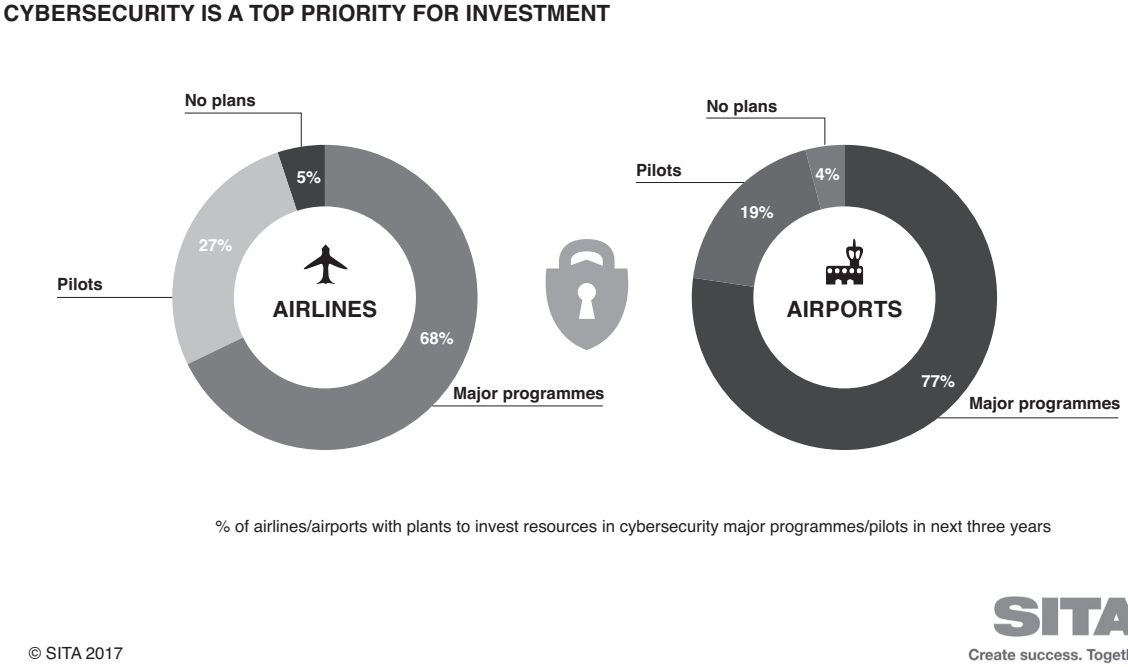

Figure 2 Investment priority for cybersecurity by airlines and airports
Source: '2017 air transport industry insights: The passenger IT trends survey', available at: https://www.sita.aero/resources/type/surveys-reports/passenger-it-trends-survey-2017.

of the ecosystem — and the ability to react to threats or actual cyberattacks in a timely and nimble way. In many parts of the global business community, this is already happening (see Figure 2).

In October 2017, the issue of cybersecurity formed the core of a keynote conference speech delivered by SITA's CEO Barbara Dalibard. She stated that, despite cybersecurity being recognised as a crucial priority by almost all airports and airlines — and despite a 46 per cent increase in the number of airlines prepared to deal with major cyber threats over the past year,[22] more needs to be done. 'We must work as a community to fight the global threat to cybersecurity,' she said. 'The industry should move from dealing with common cyber threats to being prepared for major ones.'[23]

Dalibard added: 'Airlines and airports are building their critical defenses and preparing to deal with common threats but we must all bring it to the highest level and integrate cybersecurity at executive and board level. Together we must identify, detect and react to cyber threats and protect the industry's assets from attack'.

SHARING CYBER INFORMATION

In April 2017, SITA partnered with Airbus to create a unique CyberSecurity Aviation Security Operations Center (SOC). It acts like a cyber control tower with an integrated combination of processes, people and technology to detect, analyse, respond to and report on cybersecurity incidents. SITA also operates the Community Cyber Threat Center, a security information sharing service run on behalf of SITA's 400+ air transport industry members. It enables actionable

information on cyber threats to be shared in a timely manner among key industry stakeholders.

The trickle down to the point where cybersecurity is embedded in every element of the business may still have a way to go; on a general basis, it is noted that '80 per cent of management believes they are ready to react in case of a cyber incident, but none of the technical guys agree'.[24]

Across air transport, there should be two givens. First, that security is being, or will be, breached. Secondly, that the discovery of vulnerabilities must be shared and addressed — a principle that underpins the physical safety of the aircraft and must underpin cybersecurity.

The best advice is always to assume the technology may become insecure at one point in time. It means relying on redundancy and robustness, rather than prediction and process; never connecting anything into the network without understanding what the consequences might be; avoiding risks that are not understood; and accepting that attackers are almost certainly more nimble and inventive than you are. In the words of Albert Einstein, make things as simple as necessary and no simpler. And recognise that sharing is the best antidote to a lack of resource and fear.

NEW APPROACHES TO IDENTIFYING EMERGENT THREATS

Conceivably the industry could use a healthy dose of imagination to enhance security efforts. In this unpredictable world where attackers continue to hit the 'reset' button on operational tactics, the use of imagination is crucial when identifying future threats. Perhaps the most powerful statement in the 9/11 Commission report was in Chapter 11, 'Foresight — And Hindsight'.[25] The investigators cite a lack of imagination as a root cause of the two worst attacks in US history — Pearl Harbor and 9/11. It states that: 'It is crucial to find a way of routinising, even bureaucratising, the exercise of imagination.'[26]

Of necessity, the aviation industry is tightly regulated and based on international norms and conventions. Unfortunately, but sadly not surprisingly, creative thinkers who theorise about the next attack or new threats may be marginalised, at a time when a fresh approach and out-of-the-box thinking needs to be embraced.

Asymmetric threats require an asymmetric response, and in this day and age, what we do not know is likely to be more important than what we do know when it comes to threats to the industry.[27]

It was this approach that lay behind the introduction by SITA in March 2017 of the US-based Secure Journeys Working Group.[28] The initiative was a response to a changed security climate following attacks on non-secure areas of the airport, including the Brussels airport bombing and Fort Lauderdale airport shooting. Members of the working group cite these incidents as examples that demonstrate the need to rethink the approach to getting passengers through the airport quickly and safely.

The value of Secure Journeys is its ability to bring together experts and representatives from across the air transport spectrum to provide input and recommendations based on their unique perspective and experience. Security experts from other realms will inform the group and share best practices that may be cross-applied or adapted to airport protection. Given the US Administration's focus on transportation security and commitment to large-scale investment for the nation's infrastructure, the solutions

and recommendations identified by Secure Journeys are vital to informing key decision makers.

Secure Journeys is an evolution and expansion of SITA's Border Automation User Group,[29] which was formed in 2015 to facilitate implementation of the US Customs and Border Protection's (CBP) border automation programme.

CONCLUSION

Airports face unprecedented challenges as a result of the consistent and unprecedented level of growth in passenger numbers worldwide. Air travel has never been more popular and more needed, in an ever-closer interconnected global community that is able both to enjoy the fruits of technology — and to act as a catalyst for increased innovation. But the industry also has to deal with the reverse face of that success — the global spread of terrorism as a means of political dissent, physical security and cybersecurity.

The ability of technology and the organisational skills of the industry have kept risk at a minimum, just as the industry has made air transport the safest means of transport in the world. At the same time, the evolution of working relationships with governments and their agencies — particularly where those agencies have expanded their understanding to include the whole passenger journey — has been pivotal.

But this is a continuing, evolving challenge requiring commitment, sound thinking, determination and a readiness to maintain investment in new, smarter solutions.

'We all know we need to move from conventional and mostly defensive measures to a more proactive and integrated approach with intelligence & data at its core,'[30] commented Olivier Jankovec, Director General of ACI Europe at the ACI Security & Crisis Management Summit in November 2016. 'Security measures at airports are needed — but they can only be our last line of defense. The key is to identify and stop terrorists before they ever reach an airport, or a train station or a concert hall. Because once they are there, it means we have already lost. Moving away from one-size-fits-all systematic and conventional detection towards an intelligence driven system with more deterrence and unpredictability is the only way forward if we want to deliver effective security. This implies a security culture with collaboration and data exchange at its core.'[31]

Giving her opening address to the ICAO Aviation Security Symposium in September 2017, ICAO Secretary-General Dr Fang Liu highlighted this factor: 'Aviation security remains a very dynamic context of emerging threat and risk, and we still have important challenges ahead of us. One of these is a lack of political will to set out the changes in policy and approaches now required. Some States still think that threats are other States' problems and will not occur locally. Others worry that the costs of security are not commensurate with the benefits. Still others are influenced by the perceived inconvenience on travelers. ICAO works tirelessly to confront these perceptions, but there is also a tremendous need for us to work together to foster a much deeper appreciation globally of security's importance to our sector, and to its socio-economic benefits.'[32]

References and notes

(1) UN Security Council Resolution 2309 affirms that 'all States have the responsibility to protect the security of citizens and nationals of all nations against terrorist attacks on air services operating within their territory, in a manner consistent

with existing obligations under international law.' UN (2016) 'Adopting resolution 2309 (2016), Security Council calls for closer collaboration to ensure safety of global air services, prevent terrorist attacks', 7775th Meeting, Security Council, 22nd September, available at: http://www.un.org/press/en/2016/sc12529.doc.htm; ICAO's Annex 17 SARP 2.1.2 affirms that 'Each Contracting State shall establish an organization and develop and implement regulations, practices and procedures to safeguard civil aviation against acts of unlawful interference taking into account the safety, regularity and efficiency of flights'. Annex 17 SARP 2.1.3 affirms that 'Each Contracting State shall ensure that such an organization and such regulations, practices and procedures: protect the safety of passengers, crew, ground personnel and the general public in all matters related to safeguarding against acts of unlawful interference with civil aviation; and are capable of responding rapidly to meet any increased security threat.' Available at: http://sp2010.icao.int/Security/SFP/Pages/Annex17.aspx (accessed 9th January, 2018).

(2) SITA (2017) 'Air Transport IT Trends Insights', available at: https://www.sita.aero/resources/type/surveys-reports/it-trends-insights-2017 (accessed 31st January, 2018).

(3) Airlines International (2017) 'WPS 2017: Passenger numbers set to soar', 25th October, available at: http://airlines.iata.org/news/wps-2017-passenger-numbers-set-to-soar (accessed 9th January, 2018).

(4) Airbus Global Market Forecast: 'Growing Horizons 2017–2036', available at: http://www.airbus.com/content/dam/corporate-topics/publications/backgrounders/Airbus_Global_Market_Forecast_2017–2036_Growing_Horizons_full_book.pdf (accessed 9th January, 2018).

(5) Regional Express (2017) 'Rex comments regarding regional airport security screening', 4th August, available at: http://www.rex.com.au/MediaRelease/Files/517_RexResponse-RegionalAirportSecurityScreening_4AUG17.pdf (accessed 9th January, 2018).

(6) ACI (2017) 'Policy brief: Airport networks and the sustainability of small airports', February, available at: http://www.aci.aero/Publications/ACI-Airport-Economics-and-Statistics/Policy-Brief-Airport-networks-and-the-sustainability-of-small-airports (accessed 9th January, 2018).

(7) See: http://nextt.iata.org/ (accessed 9th January, 2018).

(8) IATA Global Passenger Survey 2015 and 2016, available at: www.iata.org/publications/store/Pages/global-passenger-survey.aspx (accessed 9th January, 2018).

(9) TSA (May 2017) 'Public area security: National framework', available at: https://www.tsa.gov/sites/default/files/pass_national_framework.pdf (accessed 9th January, 2018).

(10) IATA (December 2017) 'Fact sheet: Aviation security', available at: http://www.iata.org/pressroom/facts_figures/fact_sheets/Documents/fact-sheet-aviation-security.pdf (accessed 9th January, 2018).

(11) ACI (2013) 'ACI and IATA collaborate to deliver smart security', 12th December, available at: http://www.aci.aero/News/Releases/Most-Recent/2013/12/12/ACI-and-IATA-Collaborate-to-Deliver-Smart-Security (accessed 9th January, 2018).

(12) ICAO (September 2017) 'Application of new technologies in civil aviation security of China', available at: https://www.icao.int/Meetings/AVSEC/Presentations/Session%202-Mr.%20Yan%20Li.pdf (accessed 9th January, 2018).

(13) Cohn, J., Squire, P., Estabrooke, I. and O'Neill E. (2013) 'Enhancing intuitive decision making through implicit learning'. In: D. D. Schmorrow and C. M. Fidopiastis (eds) Foundations of Augmented Cognition, AC 2013, Lecture Notes in Computer Science, Vol. 8027, Springer, Berlin, Heidelberg: available at: https://link.springer.com/chapter/10.1007/978-3-642-39454-6_42 (accessed 9th January, 2018).

(14) TSA (2017) 'Inside look: TSA layers of security', 1st August, available at: https://www.tsa.gov/blog/2017/08/01/inside-look-tsa-layers-security (accessed 9th January, 2018).

(15) PwC 'The global state of information security® survey 2018: Strengthening digital society against cyber shocks', available at: https://www.pwc.com/us/en/cybersecurity/information-security-survey.html (accessed 31st January, 2018).

(16) Whetstone, D. (2014) '"Catch the Lie": Importance of Body Language Deception Detection for Security Officials', Whetstone Security Group, Inc., WSG Inc, Sterling, VA.

(17) Catrantzos, N. (2010) 'No dark corners: A different answer to insider threats', *Homeland Security Affairs Journal*, Vol. VI, No. 2, available at: https://www.hsaj.org/articles/83 (accessed 9th January, 2018).

(18) Bunn, M. and Sagan, S. D. (2014) 'A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes', American Academy of

Arts and Sciences, Cambridge, MA, available at: https://www.amacad.org/multimedia/pdfs/publications/researchpapersmonographs/insiderThreats.pdf (accessed 9th January, 2018).
(19) See: https://www.pwc.com/us/en/cybersecurity/information-security-survey/strengthening-digital-society-against-cyber-shocks.html (accessed 9th January, 2018).
(20) Verizon (2015) 'Data Breach Investigations Report', available at: www.verizonenterprise.com/uk/DBIR/2015/ (accessed 9th January, 2018).
(21) Dubois, T. (2016) 'Thales steps up protection against cyber attacks', AIN online, 18th January, available at: www.ainonline.com/aviation-news/aerospace/2016-01-18/thales-steps-protection-against-cyber-attacks (accessed 9th January, 2018).
(22) SITA (2017) 'Air Transport IT Trends Insights', available at: https://www.sita.aero/resources/type/surveys-reports/it-trends-insights-2017 (accessed 9th January, 2018).
(23) SITA (2017) 'SITA CEO rallies airlines and airports in community fight against cyber threats', News release, 18th October, available at: https://www.sita.aero/pressroom/news-releases/sita-ceo-rallies-airlines-and-airports-in-community-fight-against-cyber-threats (accessed 9th January, 2018).
(24) Quoted in a presentation by Steven Ackx, Director at PwC, 'Protecting critical assets' at 2015 European Centre for Information Policy and Security (ECIPS) event (Antwerp, Belgium), available at: http://ecips.eu/2015proceedings/Steven%20Ackx%20-%20Enterprise%20Advisory.pdf (accessed 31st January, 2018).
(25) See: https://www.9-11commission.gov/report/911Report.pdf, Chapter 11 (from p. 339) (accessed 31st January, 2018).
(26) *Ibid*., p. 344.
(27) Hesterman, J. (2014) 'Soft Target Hardening: Protecting People from Attack', Taylor & Francis/CRC Press, Boca Raton, FL.
(28) SITA (2017) 'SITA engages aviation leaders to set new course for secure journeys at U.S. airports', News release, 16th March, available at: https://www.sita.aero/pressroom/news-releases/sita-engages-aviation-leaders-to-set-new-course-for-secure-journeys-at-us-airports/ (accessed 9th January, 2018).
(29) SITA (2015) 'Secure and efficient borders — top priority for new Border Automation User Group launched by SITA', News release, 21st May, available at: https://www.sita.aero/pressroom/news-releases/secure-and-efficient-borders-top-priority-for-new-border-automation-user-group-launched-by-sita/ (accessed 9th January, 2018).
(30) ACI news release, 23rd November, 2016, available at: https://www.aci-europe.org/component/downloads/downloads/4838.html (accessed 31st January, 2018).
(31) ACI Europe (2016) 'ACI highlights need for "more Europe" on security, during special summit', 23rd November, available at: https://www.aci-europe.org/component/downloads/downloads/4838.html.
(32) See: https://www.icao.int/Meetings/AVSEC/Speeches/Forms/AllItems.aspx (accessed 9th January, 2018).