

A secure system

Airline CEOs must set the agenda for effective security with regular health checks and programme reviews to safeguard against terrorist attacks, says John Edwards of Gates Aviation

Terrorism continues to blight our day-to-day lives and disrupt the way we do business. With each new atrocity, the media relentlessly pursues investigations into what intelligence was known by whom and when, and whether more should have been done, by governments, by enforcement authorities and often by industry, to have reduced the likelihood of the event occurring, and to mitigate the consequences of when it did.

Following each tragedy, analysis is undertaken by national security services and regulators into the terrorists' motivation, their choice of target and modus operandi. Regulators – at home and overseas – are, on each occasion, subjected to scrutiny from their political masters who seek assurance that a new attack method couldn't succeed on home-turf, and never 'on their watch'. Risk assessments are revisited. Sometimes new threats or vulnerabilities in the system are identified and new regulations or requirements follow.

Industry response

But without regard to such speculation and uncertainty, we know that commercial aviation will remain a target. We know that customers, the public-at-large and the media will watch closely to see how the industry responds. We know that current regulatory requirements have been rigorously tested (arguably, to breaking point) and serve us well; they are robust and among the best in the world. They are understood by passengers – who feel safe because of them; trusted by regulators – who know how to supervise them; and they are designed to provide solid protection against acts of unlawful interference, when properly implemented. But we do not know if they will continue to suffice. Nor do we know what the next emerging threat will be – although a group of dedicated and specialist people from across our industry work tirelessly with ICAO and other agencies to try to narrow this down.

Positive relationships

So where does that leave regional airline CEOs? Their organisations have invested heavily to embed security programmes and security management systems into their businesses. They have invested precious time and resources into building a security culture and establishing positive relationships with regulators, contractors and service and equipment providers. They have a broad range of skilled people, beyond the security team – communications, finance and industry affairs professionals and customer-facing staff all of whom make an important and essential contribution to corporate security. Their aviation security budget is already larger than they would like; they can ill-afford more cost or other additional resource-drains. What more could reasonably be expected of them?

Experience tells us that when airline CEOs demonstrate leadership in security, especially during periods of heightened



Safe-guarding against terrorist attacks needs security leaders to champion new thinking

threat, this generally inspires effective compliance within the organisation. Security leadership gives the regulator a legitimate reason to turn their focus on others – stakeholders of greater concern, or in whom the regulator has less confidence. It provides 'the leadership' with time to re-take control of the security agenda. It buys time for airlines to think about whether there are, in fact, issues that may require attention, (given the rarity of 100 per cent compliance). It creates an opportunity for the leaders to remind their political and regulatory decision-makers, overtly, of the efficacy and completeness of current security arrangements.

Everybody's business

But it also brings accountability. It is not enough to rely on the belief that airport authorities and other service providers will keep the organisation safe and secure. Security is everybody's business, but accountability stops at the highest level in the organisation. It is during periods of elevated threat, in particular, that security leaders should champion new thinking. They should adopt a terrorist mind-set and, based on this, drive re-examination of whether their security procedures could be defeated and, if so, how easily, how quickly and by whom. It is with this in mind that security leaders should insist on a security 'health-check' of their business to ensure that arrangements are fit-for-purpose and that if symptoms of security illness or vulnerability are detected, the most appropriate treatment is applied quickly. They should lead objective assessment of their company's readiness to manage the aftermath of a terrorist atrocity, if it should get caught-up in one. And from this perspective they should test and, if necessary, refresh their Emergency Response Plan.

Would such leadership safeguard aviation against the next terrorist attack? We just don't know. But effective security leadership will certainly reduce the likelihood of such an event occurring. Would it help CEOs to protect their businesses and regulators to retain confidence in the system, while they, calmly, determine their next steps? Yes, of course it would. ■