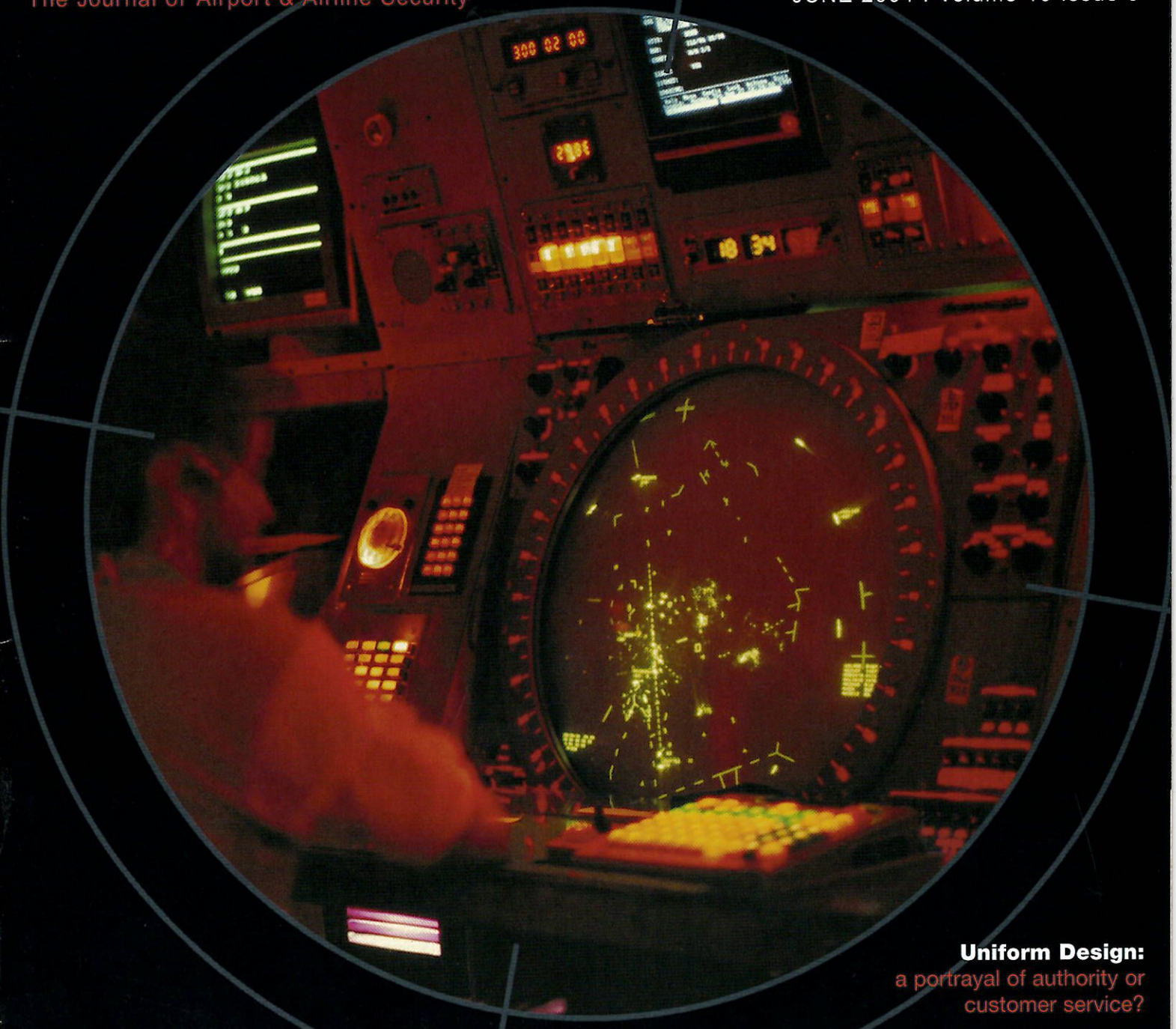
AVIATION security international

The Journal of Airport & Airline Security

JUNE 2004 : Volume 10 Issue 3



Uniform Design:
a portrayal of authority or customer service?

Blast Containment:
when all else fails

Changi & SATS:
recipe for a truly Singaporean experience

Baggage Reconciliation:
more than a question of matching bags with passengers

Air Traffic Control:
the next target?

ISSN 352-0148 USPS 010-807

SECURITY SENSITIVE OR SENSITIVE SECURITY?

BY PHILIP BAUM

It is the nature of the industry in which we work to be secretive. Preventing the dissemination of security procedures, information pertaining to criminal enquiries in progress and specific threat data is, in itself, fundamental to achieving the secure skies goal we all strive for. Quite rightly there is intelligence information that the authorities need to keep close to their chests and, understandably, there are incidences of security breaches that airports, airlines and regulators may hold back from broadcasting.

However, it also makes it all too easy for the powers-that-be to classify material as "Top Secret" due to the quality of the intelligence ascertained. The nett result is that those people on the front line – the screeners and aircrews – have little idea of either the existence of a specific type of threat or the rationale behind the new procedures they are to implement.

When governments opt not to speak of "security sensitive" intelligence, they must also recognise that the rumour mill goes into overdrive and, in the aftermath of an actual incident, conspiracy theories become the order of the day. Furthermore, when such theories are highly credible, and even proven, speculation increases that other incidents were covered up, either by the production of belated reports indicating an alternative cause for the occurrence or by the hush-hush approach.

Consider, if you will, the explosion on board TWA flight 800 in 1996. Officially the story is that a spark inside the fuel tank brought about the aircraft's demise, yet many, even with the industry, remain unconvinced. Indeed, I have spoken with a number of American government officials who still, privately, affirm that a US Navy exercise (where the target was a drone) was the actual cause. Despite such conversations, I cannot claim to know for sure the real story. I know I am supposed to accept the official report, but I also know that politics is a dirty game...

In the case of TWA 800, unless the cause of the explosion was actually an improvised explosive device, the lessons learned for aviation security are few in number. The same cannot be said, however, for the September 11th hijacks that are still shrouded in mystery.

There are so many "did you know that" stories told in whispers at industry meetings that the true aviation security practitioner is left frustrated. Meanwhile the front line screener (or crew member) is left in the dark, told to effect some additional new procedures from a revised rule book (many of which are devoid of any security common sense), and is in no way better equipped to prevent such an atrocity recurring in the future.

The stories that appear in the mass media concerning September 11th are borne out of both conjecture that breeds in the absence of the provision of real information and the nudge-nudge, wink-wink tales of those who really are in the possession of quality "security sensitive" information.

Contemplate the training advantages if it were true that the weapons used on September 11th were actually placed on board the aircraft by airport insiders rather than taken through a passenger screening checkpoint? Or, if it were true that some of the hijackers were actually in the cockpit on take-off as a result of their possessing pilots licences and able to talk-the-talk with the flight deck crews? Or, if it were true that flight UA 93 was actually brought down by Air Force intervention? Or, if it were true that a significant number of the hijackers that day had drawn attention to themselves by their strange body language?

If these were true, then our entire passenger screening response has been overkill, when it should have been our laissez-faire attitude towards staff screening that deserved the overhaul. The huge expense of reinforced cockpit door deployment would have been unnecessary. We would still be eating our meals on board with blunt metal cutlery rather than the far sharper, more hazardous, environmentally unfriendly, plastic utensils we are now given. The additional deployment of advanced screening technologies would have played second fiddle to staff training in behavioural analysis and, shock horror, we would even have to accept that a screener's gut feeling was more important than any technology's alarm signal.

By the way, on that point and as an aside, if any reader can share (on or off the record!) information as to when, if ever, an airport X-ray machine (or its operator) alone (ie. not as a result of secondary screening) has ever identified an improvised explosive device, then I'd be delighted to hear from you. It's just that considering the billions we have spent on equipping almost every airport in the world with the technology, it would be useful to have a few teaching examples that demonstrate their effectiveness for explosive detection!

I realise that, even by my writing this column, I may be fuelling further conspiracy theories. However, I don't know, with any absolute certainty, the real story (and nor do many people that think they do). What I do know is that many people who know more than I seem convinced that the aforementioned examples of "the insider story" (and many others) are true.

Most of us like to be privy to "off the record" information. Sometimes it is a matter of ego, whereby we feel that we would like to be part of that inner sanc-

tum, yet in reality we have little to gain from the extra knowledge. That said, there are many instances where by being "in-the-know", we can play our part in enhancing the security system.

Pictures, or construction information, of devices or weapons used in previous incidents are often regarded as "security sensitive" and for the trainers amongst us, we have to find devious ways of obtaining copies of them. The design of Richard Reid's shoebomb springs to mind, as does Ramzi Youssef's undetectable bomb used in the 1994 Philippine Airlines bombing, and even the home-crafted knives used by the disturbed suicidal passenger who wanted to hijack a Qantas flight to meet the devil in Cradle Mountain, Tasmania, last year. But if the trainers are not trusted, then how on earth are the screeners operating at our airports' checkpoints ever supposed to identify such an item if confronted with it in reality?

The flight cancellations fiasco earlier this year was another classic example of how the absence of information resulted in speculation and conjecture. If the intelligence itself were scrappy, then there could be little harm in saying as much. But, whatever the information available, those who actually have to effect the security procedures need also to know what they are up against. It's all very well to say that the security personnel need to be ready to handle all eventualities, with or without supporting intelligence, yet where there are specific concerns, it would undoubtedly be helpful for them to be aware.

The same would be true for aircrew who are kept even more in the dark than the screeners. Then again, there is little industry appetite to involve them. The naïve view seems to be "we must stop these incidents on the ground, not in the air". Makes we wonder why I bother having a home insurance policy – after all, I've got a burglar alarm!

There are a number of methods of aviation being attacked receiving column inches in the world's newspapers. Many a screener will be aware of such possibilities, yet cannot respond to the threat as they have not been trained to do so. Their supervisor is unlikely to know any more than them, nor perhaps their operation's senior management. Those at the top of the tree will certainly be analysing the data, all of which is "security sensitive".

Or is it? Is it not, perhaps, "sensitive security" instead? Is there not a general feeling amongst the top echelons that the nature of the threat information being received means that we have to acknowledge that we are impotent to respond to it without a total rethink and overhaul of our security approach? Heaven forbid! If the threat of a cyber attack on our air traffic control system (see lead article), or a suicide bomber detonating their device at a crowded screening checkpoint, or a chemical or biological weapons attack in-flight, or a female suicide bomber carrying their deadly cargo internally, or a TATP-based device being the order of the day thereby negating the value of many of the explosive trace detection systems, or a terrorist obtaining employment as a crewmember or mechanic were real, what defence do we have? Or is that just too sensitive a question to ask or for those who really guard us to be informed about? ■