# 9

# Aviation security culture

## Introduction

9.1     Australia's aviation security system is based on a layered arrangement. Each layer, from check-in to aircraft cabin, has a probability of failure. Increasing the number of layers and increasing the security effectiveness of each of them significantly reduces the probability of a simultaneous failure. The fact that there have been security breaches in Australia, however, even on aircraft demonstrates that the overall risk is not zero. Thankfully, Australia has not witnessed the simultaneous failure of all the layers of aviation security.[1]

9.2     While it is possible to have leading edge technology, best practice procedures, high quality training and compliance procedures, the robustness of the security system still relies on the human factor—the security culture. All aviation industry participants have a security culture and would claim it is strong—the question is, are such claims justified?

9.3     The Committee has not the resources to study in depth the security culture of the various sectors of the aviation industry, but makes the following comments based on its own observations and the evidence presented to it.

---

1     Even in the case of the attempted hijack of 29 May 2004, the cabin crew was able to contain the situation—although with the help of passengers.

The Committee believes, however, that its conclusions are applicable industry-wide.

## Security culture at small airports

9.4     The Committee has inspected facilities at two regional airports—at Coffs Harbour and Tamworth. Representatives from both airports and from Bankstown Airport also appeared before the Committee. The three airports represented, respectively: a regulated airport; a non-regulated airport servicing regular passenger aircraft; and a non-regulated airport which did not service regular passenger aircraft.

9.5     Coffs Harbour Regional Airport management told the Committee that it had a staff of four people and knew the employers at the airport fairly well.[2] This was an advantage:

> This being a small organisation, or a small community, everybody knows everybody else. Security and safety come together, and we are always conscious of strange faces and people in places where they should not be.[3]

9.6     Coffs Harbour told the Committee that it promoted a security culture through various means:

> We regularly run a terminal evacuation exercise and we take that opportunity to bring the security culture into it. … we ask that if a new employee of any company comes on line we also give them an induction, to cover ourselves under health and safety requirements but also just to give them a bit of sales talk, to introduce that culture that if you see a piece of unattended luggage you should bring it to someone's attention. I do not know how effective we are at that, because it has never really been tested, but we certainly try to keep it constantly in people's minds.[4]

9.7     The Committee asked whether there had been a major security breach at the airport. Coffs Harbour responded that there had been a person who had gained airside access, 'but he only got to the other side of the door before he was stopped.'[5]

2     Mr Bevan Edwards, *Transcript,* 2 October 2003, p. 34.
3     Mr Bevan Edwards, *Transcript,* 2 October 2003, p. 29.
4     Mr Bevan Edwards, *Transcript,* 2 October 2003, pp. 34–5.
5     Mr Bevan Edwards, *Transcript,* 2 October 2003, p. 35.

9.8     Similar evidence was provided by Tamworth Airport which told the Committee that it had a very stable workforce, most of whom had been at the airport for 13 or 14 years:

> Everyone gets to know one another around the place. If anyone wanders into an area where they should not be, they are normally challenged by the people who work there—simply because they have that safety and security culture. They are very protective of their own facilities; for example, Qantas have two large maintenance hangars and, if someone wandered into that hangar who was not known, they would be very quickly challenged by one of the staff members.[6]

9.9     Tamworth Airport agreed with the Committee when it suggested that the low risk facing the airport arose from its remoteness, the small number of people working at the airport and the small size of aircraft using the airport (jet aircraft do not fly regular services to Tamworth).[7]

9.10    Bankstown Airport only services general aviation aircraft and is not regulated. Management told the Committee that it had initiated security arrangements which were additional to that required of a non-regulated airport or for the level of risk identified for the airport. These included a person-proof fence with keypad locks, regular security patrols and a photographic identification pass system.[8]

## Committee comment

9.11    The Committee believes that smaller airports are likely to have a robust security culture. This is because the small number of employees working at such airports promotes a community attitude and allows strangers to be quickly identified. As well, there is likely to be a low level of aircraft activity at such airports which means that periods of risk are short and provides management with time to promote a security culture through training and other means.

9.12    The attitude of the airport management is also crucial, in particular, if it is prepared to initiate security requirements that go beyond the measures that are mandated.

---

6    Mr Michael Dubois, *Transcript,* 2 October 2003, p. 39.

7    *Transcript,* 2 October 2003, p. 40.

8    Mr Kimber Ellis, *Transcript,* 2 October 2003, pp. 43, 45.

## Security culture at large airports

9.13    Airport managers are the initial focus for criticisms arising from a security breach. The vast majority of workers at large airports, however, are not employed by airport management. For example, Brisbane Airport Corporation employs 130 staff, yet issues ASICs for 7 000 other employees.[9] APAM told the Committee that it had a staff of 160, but was 'accountable for an airport that has roughly 10 000 employees.'[10]

9.14    Airport managers advised the Committee that they promoted a security culture:

- through internal audits to counter complacency and keep people on their toes;[11]

- through dialogue with the unions to convey a better understanding of the outcomes being sought; and

- by signage around the airport, poster campaigns, newsletters, induction training, committees, and incident debriefing forums.[12]

9.15    More specifically, SACL told the Committee it policed very heavily the practice of people using their ASICs to 'swipe other individuals' through electronically controlled doors.[13] APAM cited the instance when it discovered that occasionally escorted visitors making deliveries to the airport were left unsupervised at the loading dock. APAM responded to the situation:

> … we put in a process where, if the escort driver had to go back to the gate because there were a number of other escorts, they simply took the person back with them and they went back to the end of the queue. So there are processes to try to address those sorts of things, but security is always about human factors. I think we have very good processes and procedures in place, but occasionally people do not always follow them. We are fairly vigilant about doing something about that if we ever discover that is the case.[14]

---

9    Mr Edward McPheat, *Transcript,* 12 November 2003, p. 55.

10   Ms Pamela Graham, *Transcript,* 21 October 2003, pp. 12, 55.

11   Mr Bevan Edwards, *Transcript,* 21 October 2003, p. 20.

12   Mr Ronald Elliot, *Transcript,* 2 October 2003, p. 27; Ms Pamela Graham, *Transcript,* 21 October 2003, p. 55.

13   Mr Steven Fitzgerald, *Transcript,* 2 October 2003, p. 20.

14   Ms Pamela Graham, *Transcript,* 21 October 2003, p. 6.

## Security incident at Melbourne Airport—a case study

9.16    On 27 July 2003 an airline passenger was 'fairly lively and vexatious'
        during check-in. The APS was called to talk to him and eventually he was
        allowed to proceed. He passed through Customs and screening without
        incident, then broke the 'break glass' alarm at doors leading to the airport
        apron. He accessed the apron through another break glass alarm.[15]

9.17    When next seen, the passenger was getting out of a vehicle at the other
        side of the airport by a ground transport officer who told personnel in a
        crewing office. Central control was advised and the passenger (who by
        now was trying on uniforms in the crewing office) was monitored until
        the APS arrived. It took two calls to central control and some 35 minutes
        for the APS to arrive.[16]

9.18    The person who challenged and monitored the passenger was a Qantas
        employee. He told the Committee that he was not involved in the debrief
        and was only offered counselling four days after the incident. The
        passenger was admitted to the psychiatric hospital at Broadmeadows.[17]

9.19    In explanation, APAM advised there were a number of alarms activated at
        the time of the incident due, it was subsequently found, to a 'cabling
        problem'. The APS initially had responded to an alarm in the wrong area.
        Even if the APS officer had gone to the correct area, APAM commented,
        he may not have seen the passenger because of all the equipment in the
        area.[18] APAM also advised that while Qantas had participated in the
        debrief, it was Qantas' decision whether or not to include the person who
        eventually challenged the intruder.[19]

## Committee comment

9.20    The security incident at Melbourne Airport highlights various aspects of
        security culture, namely:

        ■  the risks of complacency;

        ■  the need for post incident monitoring;

        ■  the risks of challenging intruders;

        ■  the need to provide feed-back and support to all involved.

---

15    Ms Pamela Graham, *Transcript,* 21 October 2003, p. 49.
16    Mr Rob Lipman, *Transcript,* 21 October 2003, pp. 32–3.
17    Mr Rob Lipman, *Transcript,* 21 October 2003, p. 36.
18    Ms Pamela Graham, *Transcript,* 21 October 2003, pp. 49–50.
19    Ms Pamela Graham, *Transcript,* 21 October 2003, p. 51.

## Complacency

9.21    APAM admitted that at the time of the incident there was a 'very high
        number of false alarms' and:

> Unfortunately, some of the staff in the coordination centre had
> lived with that for some time, and I do not think they had brought
> it to anyone's attention. … The responses may have been affected
> because there was an assumption that things were false alarms
> rather than real alarms.[20]

9.22    APAM subsequently agreed with the Committee that maintenance
        procedures now recognise security as a priority.[21]

9.23    The Committee comments that the assumption that alarms were false
        exposed a serious flaw in the security culture at the time of the incident.

## Post incident monitoring

9.24    The incident at Melbourne Airport was initially contained and apparently
        resolved when the passenger was spoken to by the APS at the check in
        area. The security problem subsequently re-emerged some time later after
        the passenger had passed through Customs and screening.

9.25    The Committee did not ascertain whether there was a procedure in place
        to monitor people after an incident to ensure security issues didn't
        reappear, or whether the system was activated. The Committee
        acknowledges that informal procedures may exist, and whether it is
        activated is always a matter of judgement of those attending the incident.

9.26    Nevertheless, the fact that the APS attended the incident should have
        raised concerns. The Committee considers that it would have been
        sensible to advise people further along the chain about the incident so that
        someone in authority was aware of the presence of a potentially disturbed
        passenger. The Committee accepts that this may indeed have occurred.

## Challenging intruders

9.27    The Committee notes that the passenger was observed in a secure area by
        a ground transport officer who did not challenge the intruder, but instead
        referred the matter to someone else.

9.28    Challenging intruders is potentially risky,[22] but is relied upon by airport
        managers:

---

20   Ms Pamela Graham, *Transcript,* 21 October 2003, pp. 49, 50.
21   Ms Pamela Graham, *Transcript,* 21 October 2003, p. 53.

> We spend a lot of time trying to promote a security culture where people do challenge if it appears that somebody is not in the right place. The issue of safety implications for staff in doing so was raised at our most recent security committee. … as the airport operator, we depend a great deal on that sort of culture prevailing, because there just is not enough APS staff on the apron to take on that accountability. So the whole notion of challenging people is fairly important to our culture, and a number of staff do it.[23]

9.29    The Committee notes that challenging may take other forms. For example, a person who overhears comments which may have security implications could either challenge directly or report the incident to the authorities. In so doing the challenger risks criticism if the security concerns are not borne out.

## Providing feed back and support

9.30    In the Melbourne Airport incident the Qantas employee involved was not debriefed and was only offered counselling several days after the event—almost as an afterthought.

9.31    The Committee considers that everyone involved in a security incident should be provided with timely feedback and support.

9.32    All employees need to be encouraged to participate in a security culture. While it may be unnecessary for a particular individual to be involved in a formal post-incident debrief, their efforts should at least be acknowledged.

9.33    Employees who challenge should not be penalised if they are mistaken. This is because such disapproval will become widely known to the workforce and will discourage the challenge culture desired by airport managers. On the other hand, over-zealous employees need to have their behaviour modified, but through sensitive and positive counselling.

---

22    On 24 July 1998 two police offers were fatally shot by a gunman who entered the Capitol building in Washington DC. The first officer challenged the intruder when he failed to walk through a metal detector; the second officer challenged the intruder inside the building. ERRI Emergency Services Report, *Shooting at US Capitol building,* 25 July 1998.

23    Ms Pamela Graham, *Transcript,* 21 October 2003, p. 54.

# Engaging the public

9.34    The Committee has received evidence on different ways in which the travelling public can become involved in aviation security, such as through signage and posters.

9.35    Qantas has suggested, however, that general airport staff and the public could become actively involved in airport security through a neighbourhood watch style of organisation. In a paper delivered at the 2003 Crime Stoppers International Conference in Melbourne, a Qantas representative said:

> We accept and encourage 'neighbourhood watch' programs, why not 'airport watch'. … We need to promote a level of security awareness across the board. … it is essential that the public at large be alert and know what to do when witnessing unusual behaviour. The taxi driver must know what to do when he overhears a suspicious conversation in his cab. The cleaner must know what to do when he witnesses some odd behaviour or locates an item that is out of place. They should all know what to report and how to report it. It is essential that we get the message across to everyone that they all have a part to play in the security process.[24]

9.36    The attitude and behaviour of airport workers will also affect the attitude of passengers. For example, members of the Committee have favourably compared the attitude of Australian aviation security screeners, among others, to the attitude of overseas airport screeners.

> **Committee**— … my own experience internationally is that the culture in our airports is more user friendly than in the United States, which is appalling. Generally, it is more comforting for passengers than I would have thought anywhere in Europe. …
>
> …
>
> **Brisbane Airport Corporation**— I have even received letters from passengers … who have been to London or New York, saying the process here is such a great experience because (a) they know they are being checked and (b) the way we facilitated it is so easy compared to overseas.[25]

---

24    Qantas, *Submission No. 77,* pp. 423, 424.
25    *Transcript,* 12 November 2003, p. 58.

9.37    BAC also told the Committee that it annually surveyed its customers, stakeholders and contractors on its performance.[26] BAC later provided the Committee with its *Quality of Service Monitoring Report* for 2003. The Committee notes that the issues surveyed included passenger comments on waiting times in various areas, the 'quality of passenger search process', and the 'efficiency of passenger search process'.[27]

9.38    At a later hearing the Committee raised the example of the courteous behaviour of Australian screening personnel as a passenger being screened set off an alarm.[28] The Committee notes in this regard, Chubb's advice that some of its clients ask that it provide supplemental training to its screeners in the areas of customer service, conflict resolution and effective communication.[29]

## Committee comment

9.39    The Committee firmly supports the view that the public should become engaged with aviation security. Such engagement will assist the public to:

■ understand fully the reasons for security and any enhanced security measures;

■ accept the inconvenience of security procedures, thereby reducing frustration and the occurrence of airport rage; and

■ gain an understanding of how to recognise potential security situations and how to respond appropriately in those circumstances.

9.40    The Committee is pleased with the friendly, yet firm, attitude of screeners in Australia. The alternative—belligerence, heavy handedness, and arrogance—as exhibited in some countries will not engage the public, and therefore will hinder security outcomes.

9.41    The Committee notes that in Australia screening services are provided by the private sector. In countries such as the USA the public sector provides screening services. The Committee draws attention to Chubb's criticism in Chapter 7 of the quality of service provided by screeners in the USA. The Committee's experiences would seem to bear out this criticism.

---

26    Mr Edward McPheat, *Transcript,* 12 November 2003, p. 59.
27    BAC, *Exhibit No. 13, Brisbane Airport Corporation Quality of Service Monitoring Report to ACCC, June 2003,* pp. 15–18, 21.
28    *Transcript,* 24 November 2003, pp. 4–5.
29    Chubb Security Personnel, *Submission No. 66,* p. 371.

9.42    The Committee believes that in the post 11 September 2001 environment passengers on board aircraft are likely to actively respond to a security incident. Other than in such extreme situations, however, response to security incidents should be left to trained professionals. Not only is this for safety and effectiveness reasons, but also to reduce the risk of compromising any legal proceedings arising from the incident.

9.43    While the Committee supports the creation of neighbourhood watch type organisations for airports, such organisations should not be extended into any form of vigilante group.

## Committee conclusion

9.44    As noted earlier, first rate equipment, training and monitoring does not guarantee a robust security culture. If the people operating the equipment and auditing performance have an inappropriate attitude then the effectiveness of security will be diminished.

9.45    The Committee suggests that a strong security culture requires an attitude which comprises:

- an awareness of, and alertness to security risks;

- a willingness to take the extra time needed to fully comply with security procedures;

- a willingness to take risks when confronted with security 'situations'; and

- a willingness to take responsibility and be accountable when security situations arise.

9.46    The Committee firmly believes management has a crucial role in allowing the attitudes listed above to flourish. Staff must be allowed to take risks—imposing sanctions against people who take risks sends a message to fellow workers that such behaviour is unwelcomed by management. It leads to a risk-averse culture which is dangerous because it stultifies initiative. The skill of management is in achieving the appropriate balance between encouraging risk-taking on the one hand and discouraging recklessness on the other.

9.47    When a robust security culture is achieved it needs to be actively maintained. Currently this is done through compliance auditing which predominantly measures skills and observed behaviour. Falling short of the required standard is met with sanctions of varying severity.

9.48    The Committee believes that there is room to encourage and support the attitudes associated with a strong security culture. Moreover, the Committee believes this can be achieved without invoking some form of sanction.

9.49    The Committee considers there is sufficient expertise available for aviation industry participants to develop ways to measure the prevailing attitude of staff to security. The Committee suggests that the use of such attitudinal surveys may be valuable in developing and reinforcing appropriate security attitudes.

9.50    It is human nature when completing a survey to wish to respond with the 'correct' answer. Therefore surveys could be designed to indicate the sorts of behaviour that are expected when security incidents arise and which are consistent with a robust security culture. Such surveys would support those who have the right attitude and encourage the adoption of correct attitudes by others. When security risks appear, there would be a good chance that the appropriate response would be made quickly and the risk would be addressed before it developed into a more serious incident.

## Recommendation 5

9.51    **The Department of Transport and Regional Services should ensure that the security programs of aviation industry participants include educational instruments designed to promote an appropriate attitude to security and, through this, a robust security culture.**

Bob Charles MP
Chairman
23 June 2004