AUSTRALIAN AIRPORTS ASSOCIATION

AIRPORT SAFETY WEEK
17-21 October 2022

DAY ONE Toolbox Talk

Insider threats at Airports

An insider is a person who exploits, or has intention to exploit, their role or knowledge for unauthorised purposes. They may be full or part-time permanent employees, individuals on attachment or secondment, contractors, consultants, agency staff or temporary staff.

The dramatic impact of an isolated few of those personnel employed within your operations could turn out to be the very people who target the industry and leave you vulnerable to an attack is known since the late '80s with the first sabotage of aircraft and is a growing concern with the rapid self-radicalisation observed in many States today.

Insider threats can take a wide variety of forms. They can be the sharing of sensitive procedures, attacks on information systems, smuggling goods or people into security restricted areas. If there is a way to cause damage or extract personal or financial gain, there is a vulnerability to an insider threat.

The danger presented by an aviation insider is that they already understand the external security of airports and aviation assets and will be able to exploit their knowledge of these security measures.

Many aviation insiders potentially also have access to the most critical and sensitive parts of an airport. They are already in a position of trust and might hold an access badge to an airport's airside, for example. Given this enhanced level of access, they are more likely to be able to identify vulnerabilities and target the weakest areas within their airport.

The motives of an insider can be varied and can include gaining financial advantage through low-level or organised crime activities. They can be issue-driven (e.g. environmentalist groups), terrorism focused, or an individual may become an insider simply because they are disgruntled or unhappy with the way they have been treated by their organisation.

While the common understanding of what constitutes an insider focuses on the 'malicious insider' who knowingly undertakes their action, an equal danger exists through the actions of the 'unintentional insider'.

Many employees by their actions leave themselves and their organisations vulnerable to infiltration or attack e.g. through the use of social engineering.

Within a dynamic environment, such as the aviation sector, these actions could potentially lead to loss of life, destruction of infrastructure, financial loss, and damage to aviation organisations. The impact of their omission or failure to comply with procedures could be equally as devastating as the impact from an insider attack.

Who could be an insider?

- Airport support staff
- Airport management or administration
- Contracted security staff
- Flight crews
- Airline agents
- Aircraft mechanics
- Baggage handlers
- Catering staff

What drive insider risk?

1. **Lack of awareness**

Staff/employees are not aware of formal policies and procedures around the emerging threat of Insider Risk within their organisations — this is particularly significant for new staff/employees.

2. **Complacency**

A relaxed or careless approach to implementing and enforcing formal policies, procedures, and security risks within the organisations.

3. **Malicious Intent**

An act that is malicious and intentional in nature — typically planned in advance that has the potential to be detected by someone else within the organisation.

Insider threat tactics

1. **Espionage**

Use of insider access to obtain sensitive information for exploitation that impacts national security.

2. **Terrorism**

Use of access to commit or facilitate an act of violence as a means of disruption or coercion for political purposes.

3. **Security Compromise**

Use of access to override or circumvent security controls (e.g. drug and contraband smuggling).

4. **Property Theft**

Use of insider access to steal material items (e.g., theft of passenger possessions or equipment).

5. **Sabotage**

Intentional destruction of equipment or material.

6. **Information Theft**

Use of insider access to steal or exploit information.

Mitigating Insider Risk

In addition to recognising your organisations vulnerabilities, mitigation approaches should form a layered approach to reducing risk and increase in complexity — these should be in addition to the deployment of counter measures that are unpredictable.

1. **Define the Insider threat —** ensure a specific working definition of Insider Threat at your organisation
2. **Define the risk tolerance -—** define the critical assets (e.g., facilities, aircraft, operations, and customer information) that must be protected and the organisation's tolerance for loss or damage in those areas.
3. **Create an Insider Threat Program —** Tailor the development of the Insider Threat Program to address your organisations specific needs, the organisation's risk tolerance, and the threat types posed. The key is to balance security with business and operational objectives.
4. **Engage stakeholders —** The program should have one owner, with input from a broad set of invested stakeholders from across the airport's ecosystem
5. **Trust, but verify —** Establish routine and random auditing of physical and logical privileged functions. Optimise the effectiveness of vetting programs and consider a periodic vetting practice.
6. **Look for precursors to Insider Threats —** behaviour-based techniques can help to identify insider threats. These observable behaviours (e.g., failed access attempts, policy violations, and undue access) can serve as potential risk indicators for proactive risk detection.
7. **Stay a step ahead —** Insiders' methods, tactics, and attempts to cover their tracks constantly evolve, which means that the Insider Threat Program should continuously evolve as well.
8. **Set behavioural expectations at your organisation —** Define the behavioural expectations of your workforce through clear and consistently enforced policies (e.g., social media, reporting incidents, and employee screening) that define acceptable behaviour.
9. **Training —** Training content should be informed by the level of physical access, privilege rights, and job responsibilities. Train your workforce to the specific insider threat risks, challenges, and responsibilities for each position (e.g., baggage handler and security screeners curriculums should vary). Embed training in onboarding processes and throughout the year.

Key Concepts of Toolbox Talk

In addition to recognising your organisations vulnerabilities, mitigation approaches should form a layered approach to reducing risk and increase in complexity – these should be in addition to the deployment of counter measures that are unpredictable.

- Risk is a factor of Threat, Vulnerability, and Consequence
- Insiders can use their unique access and knowledge to commit a malicious, complacent, or ignorant acts
- Insider risk exists in all organisations with employees and contractors
- Countermeasures are policies, programs, or tools that help prevent, detect, or mitigate insider risk

International Airport Review - Security: The hidden 'insider' threat of the aviation sector	https://www.internationalairportreview.com/article/73985/security-the-hidden-insider-threat-of-the-aviation-sector/
Journal of Air Law and Commerce - Insider Threat: The unseen dangers posed by badged airport employees and how to mitigate them	https://scholar.smu.edu/cgi/viewcontent.cgi?article=4069&context=jalc
Insider Threat	https://www.smithsdetection.com/insights/aviation/insider-threat-trends/