INSIDER THREAT IN CIVIL AVIATION

The issue and position

The dramatic impact of an isolated few of those personnel we employ within our own operations could turn out to be the very people who target our industry and leave us 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-radicalization 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.

IATA wishes to raise awareness among its member airlines and their business partners about the insider threat and proposes guidelines to establish an operator insider policy.

Background information

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

To mitigate the risks associated to this threat IATA is assisting member airlines and other stakeholders in developing, implementing and enhancing their insider threat risk identification and mitigation as part of the operator's security program, through the provision of simplistic guidance to enable operators to develop their own strategies. The guidance focused on awareness is included in this paper as well as in the IATA Security Management System (SeMS) Manual.

Objectives for Managing the Insider Threat

The objectives for developing an insider threat risk-based approach within an operator's SeMS is to:

- Provide assistance to member airlines in developing their programs;
- Provide guidance on the industry's proactive approach to addressing the insider threat.

The insider threat security risk management should be developed with the following principles in mind:

- Be security outcomes focused;
- Mainly focus on only those security measures under the management, influence and/or control of the operator;
- Reflect current operator responsibilities;
- Position the insider threat risk management within the SeMS structure, so that it becomes a part of the compliance assurance process;
- Provide a common approach, strategy and roadmap to strengthen the aviation system's resilience against the insider threat.

Insider Threat Policy

Operators need to define their policy to ensure that the appropriate procedures and processes are in place to effectively manage the insider threat. The operator will need to decide if the insider policy is to focus on terror related activity or if it will cover the full range of activities that could damage the company financially or the company's reputation such as the involvement of significant fraud.

The governance structure, including the roles and responsibilities of those involved, should be documented within the policy.

The policy should consider:

- The development of a risk assessment for relevant staff roles where exposure to risk has the potential to create significant damage to the operator;

- Insider risks to be assessed by covering scenarios considered as reasonably likely and the mitigation for such scenarios can be explored and implemented;
- Assessing the nature and magnitude of the risk and implementing proper counter-measures;
- Defining clear measures required by the operator dependent on the risk;
- Handling the insider cases at an early stage, by a member of staff, an authority, or, another third party.

Proposed solution

Pre- Employment Vetting

The policy should focus on preventing the recruitment of a person who is not able to provide a background check which is compliant with the operator's requirements. Criminal records, detailed review of employment history, travel history, correct identification etc. can provide a reasonable picture of a potential employee.

Operators should have a process to ensure that all new entrant staff complete the requirements of the vetting process prior to employment. These measures may be varied depending on the level of risk that posed by the person's role, the access to the operator's sensitive areas and activities, and the national regulations in place for background checks and vetting.

Spot and Stop Measures

Operators should consider what measures exist to identify an insider at the earliest stage and to stop or deter him.

- SPOT measures: measures aim to identify behaviors or activities of concern, and to identify any changing or suspicious behavior patterns that might help to detect a potential insider.
- STOP measures: should aim to prevent or deter an insider from exploiting, or intending to exploit their role for unauthorized purposes.

Due to changing circumstances in their lives, every person may potentially become vulnerable to being an insider, and if so, their attitudes or behaviors are significantly affected. Such circumstances range from stressful personal crises to deliberate targeting and recruitment by malicious third parties. Circumstances leading to vulnerability might be subtle and difficult to recognize. However the reality would suggest that most circumstances are caused by financial difficulty, undue pressure from peers and family, perceptions of unfairness at work, or, other inducement or coercion from third parties.

Identifying an insider is challenging. It depends heavily on other staff to report concerns about an individual and bring them to the attention of management.

The strength of SPOT measures will need to be considered by the operator and can be influenced by effective line management of personnel and the degree of effective supervision and team work. Unusual behavior is more likely to be noticed where management, supervision and teamwork is stronger. Operators will need to consider how the overall mitigation delivers the best it can for a remote workforce.

The operator should consider the effectiveness of its reporting processes[1] in regards to whether they are suitable for an employee whistleblowing on a fellow employee's behavior or where they have genuine concerns about an employee's intent. Reporting methods that are run by contracted organizations external to the operator can be considered as they enable the reporter to be anonymous, although this is not always beneficial if the investigation highlights a genuine case.

Where operators manage contractors, they may, as part of procurement activity, at least seek to be assured that the supplier has considered the insider risk, and is encouraged to deploy similar mitigation where appropriate or possible.

Communication and Awareness Measures

1 IATA Security Group developed security reporting taxonomy which should be considered when reporting insiders. If no standardized report for reporting security occurrences exists IATA report form template may be used.

One of the most effective elements in mitigating any insider risk is the awareness of the insider threat element amongst senior management and staff. For staff this awareness can be part of their vigilance when conducting everyday routines and ensuring that company processes are applied consistently to prevent or at least restrict actions by insiders.

Awareness and attentiveness are an essential layer against the insider threat. The operator should consider the provision of relevant levels of training on the insider threat to key staff groups, which can be tailored to roles as required.

Internal communications play an important part in supporting the security culture, and the insider threat should be included in such communication plans.

Response to insider activity

Where an insider has been potentially identified, either through those measures applied by an operator or when advised by the authorities, an assessment of the action required should be made.

Clearly, those of high concern, and in a high risk role, should draw an immediate and stronger response, given the industry operates to very high safety and security standards. These are difficult scenarios and it is quite possible that at the early stages the employee may have not actually infringed or broken any rules, but some level of concern exists. The response should include determining if there is a case to answer. Following these sensitive investigations subsequent investigation may be required before notifying the staff member concerned. The outcome of such investigations could involve a return to existing duties, a restriction of existing duties, or permitting the individual to seek an alternative permanent position within the roles that the operator offers recognizing a lower exposure to the concerns, or even termination of employment.

Operators should be cognizant that many apparent breaches of security have simple and possibly innocent explanations and that where possible the employee should be given the opportunity to explain their actions, but the matter should be dealt with promptly.

Any evidence of a criminal offence should be reported to the appropriate authorities at the earliest opportunity and where prosecution is a possibility, the collection of evidence should be governed by the legal requirements regarding the admissibility of information in court.

In circumstances where the information is provided to the authorities the operator will need to ensure it has the appropriate policy on how to manage the consequences of a disclosure of information regarding an employee, depending on the legislation involved.

Governance

Within the insider threat policy the operator should consider identifying a summary of the roles and responsibilities of relevant departments.