58th CONFERENCE OF
DIRECTORS GENERAL OF CIVIL AVIATION
ASIA AND PACIFIC REGIONS

Dhaka, Bangladesh
15 to 19 October 2023

AGENDA ITEM 5: AVIATION SECURITY AND FACILITATION

ESTABLISHMENT OF AUTOMATED AIRPORT EMPLOYEE SELF-ENFORCEMENT SYSTEM INTEGRATED WITH AIRPORT ACCESS CONTROL SYSTEM FOR INSIDER RISKS MANAGEMENT

(Presented by Bangladesh)

SUMMARY

This paper highlights the initiatives of Bangladesh for insider risk mitigation and the concept of an automated airport employee self-enforcement system for insider risk management using IoT (Internet of Things) and AI (artificial intelligence) in the airport access control and surveillance system as mitigation measures for the residual risk associated with insiders.

ESTABLISHMENT OF AUTOMATED AIRPORT EMPLOYEE SELF-ENFORCEMENT SYSTEM INTEGRATED WITH AIRPORT ACCESS CONTROL SYSTEM FOR INSIDER RISKS MANAGEMENT

1. INTRODUCTION

1.1 Terrorists consistently look to exploit vulnerabilities in aviation security controls in their effort to find a route of least challenge to their targets. The specific vulnerability of aviation to attacks involving the use of **insiders** in order to bypass security controls has long been understood and reflected in risk assessments and mitigation measures. However, recent terrorist attacks on aviation (**including those on Metrojet and Daallo Airlines in 2015 and 2016)** have renewed attention to the potential exploitation of those vulnerabilities and risks.

1.2 The Global Aviation Security Plan (GASeP) provides Priority Action (PA1.7) for the state to review the adequacy of current measures to address insider threat, including background checks, physical measures, training and awareness and reporting mechanisms. Accordingly, such measures need to be incorporated into the State's relevant aviation security programmes. GASeP also provides Priority Action (PA 3.2) to promote innovative techniques and technologies by States and industries.

1.3 In light of these mentioned priority actions, this paper highlights the initiatives of Bangladesh for insider risk mitigation and the concept of an automated airport employee self-enforcement system for insider risk management using IoT (Internet of Things) and AI (artificial intelligence) in the airport access control and surveillance system as mitigation measures for the residual risk associated with insiders.

2. DISCUSSION

2.1 The Insider threat. There is a growing concern in today's world that an isolated and few of our own personnel within our own operations could turn out to be a threat who has the capability to target our industry and leave us vulnerable to an attack.

2.2 Insiders are full or part-time employees (including contractors, temporary and self-employed personnel) who are working in or for the aviation sector whose role provides them with privileged access and/or knowledge to secured locations, items or sensitive security information.

2.3 The insider threat refers to the risk arising from aviation employees conducting or facilitating an AUI through the use of their authorized access.

2.4 Drivers of insider risk could range as follows:

1. **Ignorance:** Lack of awareness of policies and procedures creates risk. Employees being uninformed of policies and procedures is a challenge, particularly when dealing with emerging threats as well as new employees.

2. **Complacency:** Careless approach to policies, procedures and potential security risks. Violators often assume that their specific behavior doesn't have a noticeable impact or that no one is monitoring their behavior

3. **Malice:** malicious insiders – those who make a conscious decision to conduct an AUI – may be driven by a mix of personal vulnerabilities, situational factors, such as financial gain, ideology, revenge, desire for recognition, or coercion.

2.5 Mitigation measures: There are certain pre-existing countermeasures to insider threat built into Annex -17. In accordance with the ICAO requirement (Annex 17 Standard 4.2.3), contracting states are obliged to ensure that identification systems are established and implemented in respect of persons and vehicles in order to prevent unauthorized access to airside areas and security-restricted areas. Access to such areas shall be granted only to those with an operational need or other legitimate reason to be there. Identity and authorization shall be verified at designated checkpoints before access is allowed to airside areas and security restricted areas. Moreover, persons granted unescorted access to airside / security restricted areas must have repeatedly completed a successful background check including criminal records checks and must have received security awareness training on a regular basis. Also, airport employees are required to be screened by appropriate methods including methods capable of detecting explosives.

2.6 However, there are more mitigation measures for insider risk in best practice globally and advocated by the ICAO such as surveillance and monitoring, reporting mechanisms, behavior detection, security culture, leadership and strategy, human factors and advanced technologies.

2.7 The ongoing experiences of crime and security breaches in the airports indicate that there are still some residual security and operational risks associated with insiders such as staff involved in airport crimes (smuggling of narcotics and currencies, human trafficking, airport theft), unauthorized protocols, access to VIP areas, use of fake airport IDs, bypassing the appropriate security lane, remaining with the airport after the duty period, absent at duty place, late arrival at duty place and use expired IDs.

2.8 CAAB along with other concerned organizations are putting their efforts into controlling the above-mentioned crimes and security breaches in the airports of Bangladesh. In accordance with the ICAO requirement, and in line with SMART Bangladesh Vision 2041 and the government's zero-tolerance policy to airport security such as the adoption of a stringent policy on airport security identification system which requires enlistment of entities, certification and enlistment of designated authorized signatories of applying organization for recommending airport IDs, multi-layers of background checks, Automation of application, approval, management and verification at airport access point.

2.9 The aviation sector in Bangladesh, along with its infrastructure is rapidly growing. New, expansive airports are ready to handle a considerably larger volume of passengers, cargo and airport staff. We need to look beyond conventional ideas and ways of managing such operations. We need to rely on Innovation with technology in decision-making to manage the significantly increased passenger flow, security and operational risks arising from airport employees while considering human factors principles.

2.10 Under the initiatives of the Bangladesh Government for "Innovation in Aviation" and "Applicability and Feasibility Analysis of Various Technologies of the Fourth Industrial Revolution", an innovative idea on the establishment of an Automated Airport Employee Self-Enforcement and Insider Risks Management System was accepted.

THE CONCEPT OF AUTOMATED AIRPORT EMPLOYEE SELF-ENFORCEMENT AND INSIDER RISKS MANAGEMENT SYSTEM

2.11 This proposal provides an idea for establishing an access control self-enforcement and insider risks and operational staff management processes using AI (Artificial Intelligence: Machine Learning and Deep Machine Learning) in the airport Identification System. The system will collect data on staff behavior and movement patterns while moving within the airport and conduct an automatic risk assessment and establish interactive communication with ID users. Based on the risk assessment result, the system will require and guide ID users to maintain a self-enforcement process. This system will also facilitate authority for identifying individuals who may warrant further consideration, and/or for more in-depth assessment of individuals where concerned.

2.12 ICAO Annex-17, 15th Amendment incorporated a recommended practice to consider integrating behavior detection into aviation security practices and procedures.

2.13 Behavior detection. Within an aviation security environment, the application of techniques involving the recognition of behavioral characteristics, including but not limited to physiological or gestural signs indicative of anomalous behavior, to identify persons who may pose a threat to civil aviation.

2.14 Components and Features of the System:

1. Integrated AI-based cameras capable of behavior detection at different entry/exit and locations

2. Capable of tracking locations, calculating the time spent in different locations, and drawing movement patterns using persons and vehicle IDs using one or a combination of technologies.

3. An AI-based software with machine learning and deep machine learning algorithm that is capable of creating a unique baseline score for each person based on the provided authorization of access and the usual movement pattern for each ID holder, to calculate the deviation scores for each person.

2.15 Trigger Factors for calculating deviation will include AI Camera report, irregular pattern of movements, daily late exit report, access to unauthorized zones, time spent in vulnerable zones, unauthorized attempt for entry/exit, expired ID attempt, late entry report, time absents at duty place and early exit report, etc.

2.16 Based on the deviation score, the system will create an Interim Suspicious Staff List (ISSL) of different groups of ID users who fall under different ranges of deviation scores [ie RED (100-80), ORANGE (79-60), and YELLOW (50-40). The system will send them an electronic-Enforcement Notice through SMS/WhatsApp/Mobile App or email and will allow a sustained period for different levels of electronic-Enforcement Notice (ie 7, 10, 15 days).

2.17 Self-Enforcement and Resolution Process: e-Enforcement Notice can be resolved by self-control within the sustain period and notice can be lowered from red to orange, orange to yellow and yellow to nil. If the e-Enforcement Notice is not addressed within the sustain period, the system will automatically push in the upper list and send the e-Enforcement Notice again. When a person fails to address the e-Enforcement Notice within the sustain period of the Red List, the person will be pushed to the Permanent Suspicious Staff List (PSSL). The resolution from the permanent SSL/ISL will be resolved manually. Moreover, the frequency of recurrence in the ISSL will be calculated by the system as a deviation score.

2.18 Best Security Culture Award: In addition to the listed persons, the system will establish interactive communication with each ID holder to create awareness and provide updated information for promoting security culture. Some of the staff who demonstrates good behavior, movement and active participation in the interactive sessions and interviews may be awarded the Best Security Culture Award.

2.19 The proper usefulness of this idea lies in the technology selected for ID cards and tracking of such cards and the capabilities of machine learning. More sophisticated technology will bring more accuracy and less false results in the system. This is a primary idea. Further discussions and studies would bring more accuracy and practicality to the proposed Access Control Self-Enforcement and Insider Risks Management System.

3. ACTION BY THE CONFERENCE

3.1 The Conference is invited to:

a) note the importance of ongoing management of insider risk and mitigation of residual risks associated with insiders;

b) note the importance of innovation and technology in addressing the security and operational challenges caused by airport crimes, irregularities, and unusual movements;

c) encourage research and innovation including use of Artificial Intelligence (AI) and Internet of Things (IoT) to enhance the efficiency and effectiveness in security; and

d) share experience on the implementation of innovative solutions in future.

— END —