

Insider- An Emerging Threat to Civil Aviation

Gireeshan.P, * & Dr. Beulah Shekhar **

ABSTRACT

Civil aviation is always the silver bullet target of the terrorist due to countless favorable reason for them. After the World Trade Center attack on September 11, 2001, world countries impose stringent security norms to keep civil aviation safe and to avoid another airborne catastrophe. The amplified security measures eroded the probability of a conventional terrorist attack, and consequently, the terrorist organizations are being compelled to seek innovative ways to plan an attack. This led to the origin of an alternative form of terrorism, perpetrated by employees working inside the civil aviation or the so called insider threat. This paper provides valuable insights about the insider threat, why they are so challenging, types of insiders, their motivation, an analysis of the possibility of them being identified at the pre-attack stage, and other mitigation processes that could be utilized to ensure the safety of civil aviation.

Key Words

Civil aviation, Insider threat, Motivation, Types, Mitigation

* Research Scholar, DOCCJ, MSU, Tirunelveli, Tamil Nadu

**Professor & Head , DOCCJ, MSU, Tirunelveli, Tamil Nadu

I. INTRODUCTION

Civil aviation terrorism has a long history and it was always considered a gold standard target by the terrorist. The attack on America's prestigious World Trade Center on September 11, 2001, in which aircraft used as missile open the eyes of the world countries and more stringent security measures, with myriad technologies, processes, and layered defenses put in place to avoid further airborne catastrophe. The improvements have focused on reducing the threat primarily through managing commercial aviation passengers, including increased passenger screening, aircraft cockpit door hardening, and the vetting of civil aviation employees through various departments. But in spite of hyper-secure airplanes and air terminals, the determined terrorists will not simply give up the fight based on the fact that getting direct access to commercial aircraft as a passenger has become more difficult. Any attack on civil aviation as greatly viable in yielding important strategic destinations of terrorists which includes maximum life misfortune, financial and economic pulverization, guaranteed media scope and international publicity, terror among the citizen. Owing to these attractive reasons terrorists will begin to explore innovative methods, to carry out their attacks where they find the least resistance defeating multilayer security. One such vulnerability would be terrorist operative from an attack by an insider that has not been adequately addressed. The insiders have privileged access in and around the aircraft or aviation security information. Terrorists may utilize the opportunity to corrupt an incumbent employee in providing access or to act as an agent of the terrorist. It is a major area of concern and growing as a nightmare of security agencies.

II. INSIDER

The insider threat is one that existed as long as there have been any industries. An insider may be a current or former employee, contractor, vendor, or other business partner, who has or had authorized access to an organization's information, abilities, products, or supply chain. The knowledge or access misused to negatively affect the organization or to do harm to the public. An insider can have created a negative impact on any aspect of an organization, including employee and/or public safety, reputation, operations, finances, national security, and mission continuity. The flying industry as well isn't an exemption or secure from insider threat (Burgess, 2018).

Insider Threat a Challenge: - Why security agencies are extremely concerned about the insider threat or are considered a nightmare for them. The term insider itself embraces reason for this, they are considered as trusted agents and often do not receive the same level of scrutiny as external individuals (Loff & Wallace. R, 2014). They are often granted access credentials or security knowledge, which equip them to bypass security measures Every industry is built on the foundation of trust in the individual and most of the businesses finished up priggish and optimistic that they never stand up to such a reality of insider threats. An insider is always well versed with the external and internal security system, its gaps, and voids.

In the present the tech-savvy world the problems become more and more acute since excessive rely on technologies which include getting information on mobile devices from the off-site location as well. This increases the challenge for security as the insiders can pass the information remotely without any hindrance, exploit potential vulnerabilities, increasing their knowledge of the security systems for inimical acts. An insider with proper motivation and equipment, could plant explosives, weapons, or disable aircraft components that cause huge loss of life and property (Black, 2010). In short, insiders have substantial advantages over the external threat, and they can provide an indirect avenue for a terrorist to carry out their objective. It is a hard fact that insider threat is growing and needs more attention and should have to address without any delay. Insider threat causes billions of dollars every year globally. It is arguably the biggest threat to the global economy, global security, and critical infrastructure (Gips. & Mizell, 2020).

Aviation Insider: - Due to the vastness of airport and complexity of civil aviation multiple agencies contribute their service to a take flight in the air. Because of this unique nature potential insider threats also varies and includes airline employees, employees of airport operator, concessionaire and restaurant employees, cleaning and catering crews, construction and maintenance crews, law enforcement or security personnel, current, and former employees, current and/or former contract government employees, air traffic controllers. In the civil aviation insiders risk postures a tall degree of safety and security hazard by challenging security countermeasures, exploiting potential vulnerabilities, and expanding their information of security strategies of evil purposes. Many insider potentials have access to the most critical and sensitive installation of airports including apron area of the airport and able to identify the vulnerabilities and criticality of the various installations of the airport. It helps them to prioritize weak and strong targets.

The employees of all these agencies who have easy access and knowledge about security policies and internal matters pose a threat as an insider. In another sense, all workers from beat to foot posture danger to civil aviation as an insider. It is truly an irrefutable truth that the terrorist determinedly attempt to enroll faculty working within the flying industry with particular information of the industry (Hungerbühler, 2018).

III. INTENT

- i. Malicious:* - Insider seeks to aid or conduct an activity that is malicious and intentional in nature to cause damage.
- ii. Complacent:-* Insider takes a lax approach to policies, procedures, and potential security risks
- iii. Unwitting or Non-Malicious Insiders:* - Another category of insider threat is not malicious in motive. A poorly trained or inattentive employee can spill secrets over time as precipitously as one who intentionally discloses them (Woolley.C and Troutman.M 2013).

IV. TYPES OF INSIDER THREATS

The insider threat to the aviation sector spans across all realms of the threat vector to include terrorism, financially motivated, radicalization, revenge, mental illness, sabotage, subversion, smuggle, political cause, physical property theft, cargo, and security compromise. Some of the more notable examples of aviation insider threat across the globe include for the ibid cause are (Unknown, 2017).

- i. Terrorism:-* Use of insider access to facilitate an act of violence as a means of disruption or coercion for their wicked purposes. On 31st October 2015 Russian metro Jet aircraft departed from Sharm-El- Sheikh International Airport in Egypt exploded in midair and all 224 passengers on-board and crew were killed (Gold, 2016). Investigation revealed that the explosion was caused by an improvised bomb. After incidents, the Islamic State of Iraq and Levant (ISIL) claimed responsibility. Later reported that a mechanic at the originating airport whose cousin was a member of ISIL was able to plant the bomb. Two Airport police officers and a baggage handler were implicated, indicating the involvement of insiders (Kennedy, 2019).
- ii. Financially Motivated Terrorism:-* Rajeeb Kareem associated with British Airways(BA) used his position as an IT expert shared a lot of information including airlines and security measures with Anwar al-Awlaki, a key figure al-Qaida in the Arabian Peninsula (AQAP) who offered monetary benefit. Kareem planned a disruptive attack on British Airways accessing the BA server causing mass disturbance and monetary damage (Swann, 2011). Investigation revealed that he was determined to take a violent attack and succeeded to secure a job where he could best help the terrorists. He even tried to join as cabin crew with the aim of smuggling a bomb on board British Airways aircraft. Fortunately, his plans were thwarted (Dodd, 2011). Rajeeb Kareem was an Islamic extremist having close association with Jamat-ul-Mujahideen, an organization responsible for the terrorist attacks in Bangladesh and links with al-Qaida. It emphasized that the airlines failed to ascertain the background of the individual before inducting to the job.
- iii. Radicalized Terrorist:-* On December 13, 2013, there was an attempted suicide bomb attack detonating a weapon of mass destruction to kill as many people at Wichita Airport Mid-continent. The attack attempt was made by a radicalized avionics technician Terry Lac Loewen employed by the airport to support Al-Qaida in Arabian Peninsula (AQAP). His employment at the airport provides easy access to the airport, allowed him to study the airport layout, flight schedules. However, on D-day, he couldn't succeed in the attempt since he was under the scanner of FBI, from August 2013. Community and her

family members were stunned after hearing Loewen's plan as everyone opined he was a really good guy always calm and loving (Frosch, 2013).

- iv. *Motivated by hatred:-*** In 2007 John F Kennedy international airport (JFK) which handles approximately 1000 flights per day and 45 million passengers a year an Islamist terrorist plot to blow up the system of jet fuel supply and pipeline that the feed to the airport. The plot was foiled when an undercover law enforcement official was recruited to a terrorist cell. Two men workers were convicted of plotting an explosion of which one was a former JFK cargo worker. There was no connection to al Qaeda, but some suspects were linked to an Islamist extremist group in Trinidad (Michaud, 2007).
- v. *Mental illness:-*** Insider, a trusted employee, who suffers from a mental disorder that may not be recognized on normal conditions poses a significant risk like others who are driven by other specific motives such as money, revenge, ideology, coercion, or a simple ego. On 10th August 2018, 29-year-old Richard Russell of Horizon Air ground service agents took empty Horizon dash 8Q400 aircraft which was in maintaining position from a Seattle-Tacoma international airport and sail it for 75 minutes finally crashed, killing employees without any further casualties. Fortunately, he was with no wrong intention to hurt any more human beings. Whatever the security measure was in place could not stop him and he had passed a Transportation Security Administration (TSA) background check valid for 10 years. The incident stresses the importance of continuous evaluation procedures (Broderick, 2018).
- vi. *Sabotage:-*** Use of insider access to destroy equipment or materials . On 26th September 2014, a contractor communication technician of Chicago-area flight control set fire to the communication room at cargo Air Traffic Control (ATC). Due to thorough understanding and knowledge held by the insider, he was able to target key components to maximize the impact of the destruction. The incident caused diversion or cancellation of thousands of flights and took several weeks to put in the normal operation (Dearden, 2016). The case can be considered as the worst sabotage in the history of the ATC system and caused a **very serious** risk to aircraft safety and represents a prime example of how much damage one disgruntled contract employee can cause.
- vii. *Subversion:-*** The baggage handling staff of Rome Airport, disrupt the belt movement, to slow down the fast pace of their working to get valuable over time. During the investigation, it is found that chewing gum was stuck on the baggage bar reader and conveyor belt to slow down the speed of the belt. The passenger waited for a long time to reclaim their baggage or at worst had not found their bags and puts the whole airport in crisis (Kington, 2007).

- viii. Smuggle:-** A former Delta Airlines baggage handler was sentenced to 30 months for allegedly smuggling guns on passenger planes. Eugene Harvey a delta baggage handler used his security badge broke the airport security to smuggle gun to the restricted area of the Atlanta airport. At the restroom, Harvey transferred the firearms to the formal Delta employee who hid the gun in carry-on baggage and took them into flights from Atlanta to New York. The gun was illegally sold in New York. He trafficked a total of 135 firearms between Georgia and New York without any concern for the safety of airline passengers (Hoggan, 2019).
- ix. Political Cause:-** The Co-pilot namely Hailemedhin Abera worked for Ethiopian Airlines for five years without any Criminal background took over control of the flight of its fly to Rome from Ethiopian capital Adis Ababa while the pilot took a toilet break. The Ethiopian Co-pilot sought political asylum in Switzerland. Although the flight landed safely at Geneva Airport without any harm to passengers and crews it exposes another possible method from the insider. Although the incident has no significance from the point of terrorism, it throws light on a rare case in which pilots hijacking an airplane (Penketh, 2014).
- x. Physical Property Theft:-** Insider access to steal material items. In late August 2016, a united airline employee was arrested and charged with on account of felony theft for allegedly stealing \$130,000 worth of jewelry from a passenger's bag in the U.S. airport. During the investigation, the video from the airport's surveillance system shows the employee taking possession of the cosmetic case and intentionally wrapping the case with a piece of paper at the gate. The incident highlights the high handiness of airlines employ in theft cases(Unknown,2017).
- xi. Cargo:-** Although incidents in which using cargo as means to place explosives and other malicious activity are very rare, stringent security measures on passenger aircraft since the 9/11 attack could make cargo aircraft and cargo operation make more attractive for the terrorist. Incidentally, most of the crime-related to cargo operation committed with the connivance of cargo workers. Therefore, this is another area of growing concern for the security agencies and which is different from the passenger operation. An off-duty Federal Express flight engineer attempt to hijack an aircraft intended to crash on companies headquarter. As he was authorized free access to aircraft, exploit the exemption from security screening. He concealed hammers, mallets, a knife, and a spear gun in his only luggage, a guitar case. The hijacker boards the aircraft under the pretext of travel to San Jose, California. Even though the flight crew foiled the hijacker's attempt, the incident throws the light on the susceptibility of cargo flight (Elias, 2007).

VI. IDENTIFYING THE INSIDER THREAT

The number of insider attack cases brought insider threats to the forefront of public as well as security agencies. The above incidents are selective and indicative of only those which show the current paradigm of insider threat. This contour does not represent all cases. There are a large number of incidents where insiders used their special airport access for unlawful interference in civil aviation. It is significant to note that there is no conclusive technique to identify insider threats before they strike, nor is there any way to completely prevent the damage they can inflict (Woolley & Troutman.M 2013).

Several indicators of insider threat known by human resource staff to raise a high level of concern include but are not limited to performance, stress, self-centeredness, and personal issues. While calculating the psychosocial risk of insider threat, these indicators carry different weights. Unlike other industries due to the active involvement of multiple agencies, civil aviation is susceptible to a great degree of probability from insider threat. Due to changing circumstances and radical transformation in international developments, every employee is susceptible to insider threats. If so, their attitude, approach, and behavior may vary from regular ways. Such conditions may vary from stressful personnel crisis to detach. Circumstances leading to vulnerability might be subtle and identifying those is a herculean task. It depends heavily on peers, effective management of personnel, close supervision, multiple party monitoring, and finally synergy among the team members. Each operator should consider what measures exist to identify an insider at the earliest stage and prevent further aggravation.

Adverse online behavior: - Adverse online behavior can be defined as the activity of a person in an electronically mediated format. It involves a person's interaction with online media or interaction with other people participating in electronically mediated behavior (Woolley & Troutman.M 2013). It focuses on the interpersonal behavior of people while they are online which includes their self-representation, and any anti-social behavior.

VII. MEASURES TO MITIGATE INSIDER THREAT.

It is really unfortunate that there is no stand-alone arrangement to annihilate insider danger. It needs a coordinate framework, persistent overhauling of the procedures (Woolley & Troutman.M 2013). Considering complexity and variety of the threat and indistinguishable motives of the insider as discussed above, a wide range, multi-pronged approach are the sine qua non to root out insider threat. The organization assiduously modernizes its policy to ensure appropriate procedures and processes are in place to manage insider threats effectively including background checks, physical measures, training, awareness and reporting mechanisms. The organization decides whether its insider policy effectively controls terror-related acts or else it will cover the full range of activities that could hamper the organization's reputation in different ways (Unknown, 2018). Understanding past flying insider danger occasions likely help in fortifying proactive security measures, instead of responsive reactions. In

spite of numerous layers of security input there's continuously room for enhancement in ensuring gracious flying, in securing against insider danger (Krull, 2016).

VIII. CONCLUSION.

The insider threat is one that has existed as long as there have been aviation industry employees and one that will always be a component of the industry. However, it attracts the attention of security agencies and comes to the forefront after the various blatant incidents. The above anecdotes are indicators only and contours are not limited there. Security agencies are always trying to improve the system incorporating new technologies and measures to plug the loopholes in the existing system but at the same time terrorist always try to break the system by hook and crook which is evident from the above examples. It is not possible to handle such a versatile threat by stand-alone measures but demands a multipronged, multifaceted approach. In conventional aviation security and its rapid overhaul after the 9/11 attack importance is given to passenger screening and little importance is given to threats from the insider. This may due to the complacent of the organization as they considered their employees are trusted, once they are inducted and give leverages to perform their duties and permission to access sensitive areas (Nessi, 2018). But threat perception is changing rapidly. The repercussion of any failure in the civil aviation security unfathomable and its reverberation is beyond the imagination. This mandates new approaches, procedures, regulations, need for strong security culture, and internal counter check measures without bothering the convenience of the employees who may take such measures as a nuisance. Aviation security is something that cannot be achieved in isolation. It needs a comprehensive risk-based security strategy and delivered consistently by all stakeholders, law enforcement agencies, regulators, and operators. Unfortunately, there is no silver bullet to eliminate insider threat, it constantly evolves. As history has proven, disastrous consequences may follow from abuse of the freedom given to airport badge holders. While the overall security of the system today is significantly better than on September 11, 2001, and before, it is clear that there is still a lot of work that must be done in order to ensure that the security of commercial aviation continues (Greco, 2017). In short, it is the responsibility of the individual organization to protect civil aviation from any unlawful interference for that they have to adapt all means and its continuous evaluation, risk assessment keeping the system dynamic, flexible, and unpredictable to make zero error.

References

1. Black, A. (2010). *Managing The Aviation Insider Threat*. Monterey, California: Naval Postgraduate School.
2. Broderick, B. C. (2018). Taking Stock of the Insider Threat. *Aviation Week Network*.

3. Burgess, C. (2018). *Aviation industry takes steps to mitigate insider threats*. Framingham, MA: CSO.
4. Woolley, C and Troutman, M. (2013). *Insider Threat: Policy Impact And Overview. Insider Threat Workshop Proceedings* .
5. Dearden, L. (2016, February 24).
Retrieved April 19, 2020, from <https://www.independent.co.uk/news/world/africa/isis-plane-attack-egypt-terrorists-downed-russian-metrojet-flight-from-sharm-el-sheikh-islamic-state-a6893181.html>.
6. Dodd, V. (2011, February 28).
<https://www.theguardian.com/uk/2011/feb/28/british-airways-bomb-guilty-karim>.
Retrieved April 20, 2020
7. Elias, B. (2007). *Air Cargo Security*. Washington, DC: Congressional Research Service.
8. Frosch, D. (2013, December 13).
Retrieved April 20, 2020, from <https://www.nytimes.com/2013/12/14/us/man-accused-of-airport-bombing-attempt-in-kansas.html>.
9. Gold, Z. (2016). *Egypt's Aviation Security since the Metrojet Bombing. ICCT*.
10. Greco, J. P. (2017). *Insider Threat: The Unseen Dangers Posed by Badged Airport Employees and How to Mitigate Them. Journal of Air Law and Commerce*.
11. Hoggan, K. (2019). *Insider and their threat to Aviation Security. H4 Solution*.
12. Hungerbühler, F. (2018). *Uniting Aviation*. Montreal: ICAO EUR/NAT .
13. Loof, J and Wallace, R. (2014). *The unmitigated insider threat to aviation. Journal of Transportation Security*.
14. Gips, M and Jr, Mizell. (2020). *Inside the Insider Threat*. W. Big Beaver Rd, Suite: Security Magazine.
15. Kennedy, K. (2019). *Aircraft Security: Protection from the Insider Threat. Aviation Security International*.
16. Kington, T. (2007, August 6).
Retrieved April 12, 2020, from
<https://www.theguardian.com/business/2007/aug/06/theairlineindustry.italy> n.
17. Krull, K. (2016).
The Threat Among Us. Richland, Washington: Pacific Northwest National Laboratory.

18. Michaud, C. (2007). Four charged in plot to blow up JFK airport. Reuters.
19. Nessi, D. (2018). Is the Aviation Industry Prepared to Manage the Insider Threat. *Connected Aviation Today*.
20. Penketh, A. (2014, February 17).
Retrieved April 24, 2020, from <https://www.theguardian.com/world/2014/feb/17/copilot-arrested-hijacking-ethiopian-plane>.
21. Swann, S. (2011, February 28).
Retrieved May 1, 2020, from <https://www.bbc.com/news/uk-12573824>.
22. Unknown. (2017). *Aviation Insider Threat: What We Know, Our Findings, and What We Recommend*. The Public-Private Exchange Program.
23. Unknown. (2018). Insider Threat and Security Culture. *Second High-Level Conference On Aviation Security*. Montréal: International Civil Aviation Organization.