INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN ECONOMICS & MANAGEMENT SCIENCES

OPEN ACCESS JOURNAL

Vol 14, Issue 2, (2025) E-ISSN: 2226-3624

Unlawful Interference and Airport Economics: A Conceptual Framework for Enhancing Employee Awareness at Abu Dhabi International Airport

Amer Ali Saeed Alnuaimi
Universiti Teknikal Malaysia Melaka
Email: Uae-alnuaimi@hotmail.com

Sabri Mohamad Sharif
Universiti Teknikal Malaysia Melaka, Faculty of Technology Management and Technonpreneurship
Corresponding Author Email: sabri@utem.edu.my

To Link this Article: http://dx.doi.org/10.6007/IJAREMS/v14-i2/25287 DOI:10.6007/IJAREMS/v14-i2/25287

Published Online: 22 May 2025

Abstract

Abu Dhabi International Airport (AUH) serves as a critical global aviation hub, facilitating economic growth in the UAE through tourism, trade, and connectivity. However, its strategic importance also makes it vulnerable to acts of unlawful interference such as attacks on passengers, infrastructure sabotage, and misinformation which pose immediate safety risks and long-term economic consequences. Guided by Routine Activity Theory (RAT), this study propose a conceptual framework that examines how employee awareness of unlawful interference impacts airport economic performance. The finding of this study revealed that four key areas: flight delays/cancellations, tourism disruptions, stock and investment volatility, and maintenance/repair costs are at the top of the employees awareness factors that influence airport economic performance. Additionally, the study investigates the moderating effect of managerial security procedures on enhancing employee awareness to counteract these threats. The research proposes a conceptual framework that synthesizes existing knowledge on unlawful interference dimensions, regulatory frameworks (e.g., ICAO, IATA, GCAA), and economic impacts, while hypotheses are developed to test the relationships between awareness, managerial procedures, and economic resilience. The findings aim to provide actionable insights for strengthening airport security protocols, optimizing resource allocation, and safeguarding Abu Dhabi's aviation-dependent economy. By bridging theoretical and practical perspectives, this research contributes to the discourse on aviation security and offers strategies to bolster AUH's resilience against evolving threats.

Keywords: Conceptual, Framework, Awareness, Unlawful Interference Abu Dhabi, Airport

Introduction

Abu Dhabi International Airport (AUH) serves as a vital global aviation hub, bridging the East and West while significantly contributing to the UAE's economic growth through tourism, hospitality, and financial sectors (El Naggar & Abdelrazik, 2024). However, its strategic importance also makes it a prime target for unlawful interference, including passenger attacks, infrastructure sabotage, and misinformation campaigns (Al Jasmi, Mohd Udin, & R. A. Siam, 2021). Such threats not only jeopardize immediate safety but also have far-reaching economic consequences, disrupting airport operations, damaging reputation, and destabilizing the broader economy. Addressing these vulnerabilities is critical, and enhancing employee awareness emerges as a key strategy for risk mitigation. Grounded in Routine Activity Theory (RAT), this study underscores the necessity of a vigilant workforce capable of identifying and neutralizing threats before they escalate (Hanus & Wu, 2016). By fostering a security-conscious environment, AUH can minimize operational disruptions, reduce costly damages, and sustain economic stability.

The economic repercussions of passenger-targeted attacks are particularly severe, as they erode public trust in airport safety and deter travelers, leading to potential declines in tourism and airline revenues (Sun, Wandelt, & Zhang, 2020). Given AUH's role as a major transit hub, any security breach could trigger widespread disruptions across the aviation network. Employee preparedness is crucial in such scenarios—trained personnel can swiftly detect and respond to threats, mitigating their impact and maintaining passenger confidence (Al Jasmi, Mohd Udin, & R. A. Siam, 2021). Similarly, infrastructure attacks impose heavy financial burdens, necessitating unplanned repairs and straining operational capacity (Sun, Wandelt, & Zhang, 2020). The 2020 drone incident at AUH highlighted the importance of employee readiness in ensuring rapid recovery and preventing prolonged disruptions (Burlov et al., 2022). A well-trained workforce not only enhances security but also optimizes resource allocation, reducing maintenance costs and preserving seamless passenger flow.

Misinformation presents another formidable challenge, with the potential to inflict lasting economic damage by undermining Abu Dhabi's reputation as a safe travel destination (Al Jasmi, Mohd Udin, & R. A. Siam, 2021). False claims about security threats or operational failures can lead to canceled bookings, reduced tourist inflows, and financial losses across the hospitality sector. Empowering employees to counteract misinformation through clear communication and prompt clarification helps stabilize traveler confidence and safeguard economic activity. Flight delays and cancellations, often immediate consequences of unlawful interference, further amplify financial strain by increasing operational costs and disrupting connecting flights (Calzada & Fageda, 2023). A knowledgeable workforce is essential in minimizing these disruptions, ensuring efficient incident management, and maintaining AUH's reputation for reliability (Wandelt & Wang, 2024). Beyond operational impacts, unlawful interference affects Abu Dhabi's tourism-dependent economy, where AUH serves as the primary gateway for international visitors (Rashad et al., 2024). Perceived insecurity or frequent disruptions may divert travelers to competing hubs, diminishing tourism revenues and affecting ancillary industries. Employee awareness and preventive training play a pivotal role in reinforcing Abu Dhabi's image as a secure and welcoming destination. Additionally, security incidents can trigger volatility in aviation and tourism-related stocks, undermining investor confidence (ATAG, 2018). A workforce proficient in threat response demonstrates AUH's resilience, reassuring investors and sustaining economic growth.

Managerial security procedures further enhance the effectiveness of employee awareness by providing structured protocols for threat mitigation (Alards-Tomalin et al., 2014). Clear guidelines, emergency drills, and compliance with international standards ensure that employee preparedness translates into decisive action, minimizing economic fallout (ATAG, 2018). This study proposes a conceptual framework to examine how employee awareness of unlawful interference spanning passenger attacks, infrastructure threats, and misinformation—influences AUH's economic stability. By integrating RAT and emphasizing the moderating role of managerial procedures, the research offers actionable insights for strengthening airport security and sustaining economic resilience in an increasingly complex threat landscape.

Literature Review

Acts of Unlawful Interference

(Teichmann, Boticiu and Sergi, 2023), describes the acts of unlawful interference as practices to jeopardize safety and security on any place, it aims to deliberately attack companies, firms and organization to impact the overall security. It might attack systems, people, networks, confidential data and so on and so forth (Buchan, 2012).

Its influence not only has a minor impact or temporary damage, but also may last for a long-time and result in long-term harm and depression (Hollerer, Sauter and Kastner, 2022). In other words, it is by nature an illegal intervention by an external factor that can break the rules or could be an internal factor that is unauthorized by law to perform that kind of practice which could lead to minor or major dilemma (Pham and Xiong, 2021). That is highlighted by many multinational and international establishments, as everybody believes, the bigger size of the company, the greater chance of unlawful interference is likely to happen (Pavelenko, 2018).

Besides, such acts consist of terrorist attack, hijacking, stealing, cyber security crimes, armed robbery, bombing self or establishments, accessing restricted zones and so on and so forth (Siadkowski, 2014). While Siadkowski (2014) defines the acts of unlawful interference as the acts of trying to do whatever harmful that could jeopardize the safety and the security of people and infrastructure and could put the full civil aviation system at risk.

Act of Unlawful Interference on Civil Airports

Civil airports are designed to facilitate the movement of passengers and cargo, serving as vital hubs for global connectivity and representing the reputation and economic stability of their respective countries (Agustini et al., 2021; Duchesneau, 2017). Airports are complex ecosystems involving numerous stakeholders, including ground handling personnel, airline staff, customs and immigration officers, and civil aviation employees, all critical to ensuring seamless operations and maintaining safety (Ogonowski et al., 2020). Beyond their logistical role, airports symbolize national pride and act as gateways to cities worldwide (Duchesneau, 2017).

The critical nature of airports makes them prime targets for unlawful interference, such as sabotage, hijacking, ground attacks, cyberattacks, and the use of improvised explosive devices (IEDs) (Duchesneau, 2017). These threats jeopardize not only safety and security but also the broader economic and political stability of nations. The involvement and awareness of

employees at all levels are paramount in detecting and mitigating such risks. Employees who are well-informed about potential threats and trained to respond effectively can serve as the first line of defense, significantly reducing vulnerabilities and enhancing overall airport resilience.

The International Civil Aviation Organization (ICAO) and national civil aviation authorities are tasked with implementing robust security strategies, contingency plans, and legal frameworks, such as the Tokyo, Hague, and Montreal conventions, to counter these threats (Abeyratne, 2018). While these conventions address issues like aircraft seizures, sabotage, and attacks on airport systems, their effectiveness relies heavily on the active participation and readiness of airport employees. However, the lack of standardized security measures across nations remains a challenge, underscoring the need for global collaboration and consistent training (Agustini, 2021). Historical data highlights the magnitude of the problem. Between 1931 and 2016, incidents such as hijacking (1,308 cases), ground attacks (536 cases), sabotage (174 cases), and suicide missions (53 cases) resulted in thousands of fatalities and widespread infrastructure damage (Duchesneau, 2017). These acts not only threaten civil aviation but also disrupt supply chains, destabilize economies, and amplify terrorist agendas (Ogonowski, 2020; Duchesneau, 2017).

Given the stakes, enhancing employees' awareness and preparedness is critical. Well-trained personnel can identify early warning signs, ensure proper implementation of security protocols, and minimize the impact of unlawful interference. This proactive approach, coupled with international collaboration and strengthened infrastructure, is essential to safeguarding airports, protecting national reputations, and ensuring the economic viability of the aviation industry.

International and Local Association Regulating Civil Airport Security

It is very notable that the civil aviation industry is led by a respected local and international authorities, the purpose of those authorities is not only regulating the travel industry, but also set a rigid guidelines and procedures that can impress the aviation community world wild from operational and security perspectives. In this part, the researcher will mention and discuss the main leading associations such as ICAO, IATA and GCAA.

ICAO (International Civil Aviation Organization)

The International Civil Aviation Organization (ICAO) is a highly esteemed organization that has made invaluable contributions to the aviation industry by establishing overarching guidelines and protocols (Abeyratne, 2024). It provides local authorities with the latest international updates on operations, safety, and security, forming a foundation for enhancing global aviation standards (Agustini, 2021). ICAO plays a pivotal role in advancing aviation security through several key initiatives. As outlined by Agustini (2021), these include the development of Annex 17, which provides detailed practices to counteract acts of unlawful interference. ICAO also ensures the implementation of all international security conventions, delegates essential tasks to local authorities such as airports, airlines, or police agencies, and defines the roles and responsibilities of agencies tasked with providing security infrastructure. Additionally, it promotes the adoption of the Reason Model for airline security, emphasizing a systematic approach to identifying and mitigating vulnerabilities.

A critical aspect of aviation security is the awareness and preparedness of employees within the aviation sector. While ICAO provides robust protocols and frameworks, their success is significantly influenced by the level of awareness, training, and readiness of airport employees. Employees serve as the frontline defense against security threats, and their ability to recognize potential risks, respond effectively to emergencies, and implement security measures is crucial. Continuous training programs and educational initiatives focused on ICAO guidelines are essential for ensuring employees are equipped to handle diverse security challenges (Abeyratne, 2024). Empowering employees with knowledge and skills not only enhances the implementation of security measures but also fosters a proactive security culture that can prevent or mitigate the impact of unlawful interference. Moreover, ICAO mandates that every construction state ensures the optimal implementation of airport security infrastructure (Sulmona, 2015). Privatized airports and associated agencies are also required to liaise with ICAO and adhere to both its guidance and local state security regulations (Sulmona, 2015). These efforts underscore ICAO's extensive influence on aviation and civil airport security procedures and protocols, highlighting the critical role of employees and unified global standards in maintaining safety, security, and resilience in the aviation industry.

IATA (International Air Transport Association)

The International Air Transport Association (IATA) is regarded as a pivotal organization in the aviation sector, often described as the "godfather" of the industry due to its extensive contributions to airline operations and security (Yu, 2020). According to Sulmona (2015), IATA has a major impact on civil aviation security, providing guidelines and frameworks to enhance safety and efficiency. Among its key contributions, IATA emphasizes that every state is primarily responsible for ensuring security within its jurisdiction. Governments play a critical role in supporting civil airports by offering cost-effective and efficient security solutions, providing airlines with adequate financial information, and consulting airlines on security measures. Additionally, IATA advocates for a shared responsibility between states and airlines in bearing the costs of implementing security systems. Tyler (2016) highlights that IATA has taken further steps to support the aviation security industry by proposing innovative initiatives such as the Smart Security System. This system aims to enhance security measures while improving passenger convenience and operational efficiency. IATA not only assists states in embedding robust security rules and regulations but also monitors these measures to ensure compliance (ZAG, ALS and INOV, 2021). The organization actively alerts states and airlines to any deficiencies in their security systems, emphasizing the need for continuous improvement.

A critical element of IATA's security initiatives is the awareness and involvement of employees within the aviation sector. Employees play a frontline role in implementing and upholding the security measures proposed by IATA. Ensuring that personnel are well-trained, informed, and vigilant about potential risks is essential to the success of these measures. Through ongoing training programs, awareness campaigns, and collaboration between airlines and governments, IATA fosters a culture of proactive security readiness among employees. This awareness not only enhances the effectiveness of implemented security systems but also mitigates potential risks, safeguarding both passengers and aviation infrastructure. By bridging the gap between policy and practice, IATA ensures that employees are a cornerstone of its comprehensive security approach.

GCAA (General Civil Aviation Authority)

Two prominent international civil aviation associations, the International Civil Aviation Organization (ICAO) and the International Air Transport Association (IATA), play crucial roles in establishing, recommending, and monitoring security rules and procedures for the aviation industry. These organizations emphasize the importance of international collaboration in developing security standards while underscoring that the ultimate responsibility for implementing and enforcing these measures lies with local authorities and the state of origin. In the United Arab Emirates (UAE), the General Civil Aviation Authority (GCAA) fulfills this critical role. The GCAA serves as the main regulator for the UAE's aviation sector, tasked with ensuring compliance with operational, safety, and security standards. As per the General Civil Aviation Authority (2024), the GCAA enforces a range of security measures, including requiring all operators to adhere to the national security program and clarifying specific security requirements for airports and airlines. It also identifies and categorizes potential security threats, establishes aviation security tasks, and monitors security practices to maintain safer aerodrome facilities. Furthermore, the GCAA actively disseminates updated information about emerging security issues to its partners and integrates a comprehensive security alert system. Another critical function of the GCAA is training relevant personnel to handle acts of unlawful interference effectively, including responding to bomb threats or other emergency scenarios. By equipping employees with the necessary knowledge and skills, the GCAA ensures a proactive approach to mitigating risks and enhancing security readiness. This dual emphasis on robust regulatory frameworks from ICAO and IATA, combined with the localized implementation and enforcement by authorities such as the GCAA, underscores the interconnected nature of global and local aviation security efforts. Through its stringent measures and focus on employee awareness, the GCAA contributes significantly to safeguarding the UAE's aviation sector and maintaining its resilience against evolving security challenges.

The Components of Civil Airport (Fixed Variables)

Civil airports are complex systems comprising multiple interconnected elements that collectively shape their overall structure and functionality. When discussing civil airports, several components often come to mind, including terminals, concourses, screening areas, passengers, planes, airside operations, and landside facilities (Abeyratne, 2018).

Among these various aspects, the focus here is on three core components that are fundamental to airport operations: passengers, planes, and airport infrastructure. These elements are integral to understanding the dynamics of civil aviation and its impact on safety, security, and efficiency.

Passengers

Passengers are broadly categorized into two primary groups: joining (local) passengers and transfer passengers, with both further divided into domestic and international subcategories (Marteache, 2013). Joining passengers are those who begin their journey from their origin or base and travel to a destination that serves as their final point of disembarkation. In contrast, transfer passengers are those who pass through one or more airports to reach their final destination, often using multiple flights or airlines. The need for transfer passengers to change flights may arise due to the unavailability of direct routes, extended distances, or cost

advantages, as transfer tickets are often cheaper than direct flight options (Robert, 2006; Marteache, 2013).

Domestic passengers travel within the same country, moving from one city to another, such as a journey from Washington D.C. to Los Angeles in the United States. On the other hand, international passengers fly between cities in different countries, such as traveling from Abu Dhabi, UAE, to Kuala Lumpur, Malaysia (Marteache, 2013). Another categorization of passengers, introduced by Wan (2015), distinguishes between business passengers and leisure passengers. Business passengers typically travel for short durations to attend meetings, exhibitions, or oversee business operations in different locations. In contrast, leisure passengers travel for holidays or tourism, often for medium to long durations, with the aim of exploring destinations and visiting attractions (Wan, 2015). Understanding these passenger categories is crucial from a security perspective. Differentiating between passenger types enhances the ability to predict and prevent acts of unlawful interference targeting them. This foundational understanding provides insights into how attacks on passengers might occur, a topic explored in greater detail in other sections of the literature under the theme of "attacks on passengers."

Planes

Airplanes, also referred to as aircraft or planes, are the primary means of transportation in civil aviation, enabling fast travel across vast geographical distances (Gössling and Humpe, 2020). Civil aircraft are utilized for various purposes, including transporting passengers, cargo, and couriers, often serving multiple functions simultaneously. According to (Verde, 2024), civil aircraft are broadly categorized into two types: narrow-body aircraft and wide-body aircraft.

Narrow-body aircraft feature a single aisle running through the center, flanked by rows of seats on either side. These aircraft typically accommodate 50 to 200 passengers. Common examples include the Boeing 737 series and Airbus A320 and A321 models (Vadaparthi, 2017). In contrast, wide-body aircraft are larger, with two aisles separating three seat sections left, middle, and right allowing for greater passenger and crew movement. These planes typically carry between 250 and 600 passengers and, in some cases, include two decks, providing additional capacity and comfort. Examples of wide-body aircraft include the Boeing 777 and Airbus A380 (Lee et al., 2022). Understanding the types and capacities of aircraft operating at an airport is a critical responsibility for all personnel in the civil aviation industry. This knowledge is essential for ensuring operational efficiency, safety, and security. Employees who are aware of aircraft specifications can better manage passenger flow, cargo handling, and emergency protocols, thereby enhancing overall airport operations. Furthermore, employee awareness about aircraft types is vital for identifying potential security risks and implementing tailored measures to address them. By fostering a well-informed workforce, civil aviation authorities can ensure smoother operations and mitigate risks associated with the diverse range of aircraft taking off and landing at their airports.

Airport Infrastructure

Airports are fundamentally divided into two major components: landside and airside. The landside includes all areas accessible to the public before crossing the immigration checkpoint. These areas comprise car parks, transportation networks, metro station access

points, curbsides, check-in areas, restaurants, service shops, ticketing offices, and passenger terminals (Dimitriou, Sartzetaki and Karagkouni, 2025). Regulated car parks for passengers, visitors, and staff are often connected to passenger terminals, with curbsides serving as transitional zones between car parks and terminal entrances. Terminals themselves are critical hubs, facilitating the movement of passengers from curbside to check-in processes. Check-in areas involve identity verification, baggage weighing, and security screening by check-in agents (Skorupski, Uchroński and Łach, 2018).

The airside, on the other hand, begins after crossing immigration and is accessible only to checked-in passengers or authorized personnel. This area encompasses concourses, transfer desks, screening zones, restaurants, lounges, gates, aerobridges, aircraft parking areas (aprons), runways, taxiways, and control towers (Richard de Neufville and Odoni, 2013). Concourses are typically elevated structures allowing passengers to move freely or relax before proceeding to gates. Gates serve as the final interaction point between passengers and airline staff, leading to aerobridges or transfer buses to the aircraft.

The apron is a critical operational area where essential activities such as loading, unloading, fueling, catering, and aircraft maintenance occur. It is surrounded by ground service roads and supports a variety of safety and operational vehicles. Runways and taxiways are equally vital, serving as the areas for aircraft takeoff and landing. Runway length is a significant factor in ensuring safety, as longer runways provide sufficient space for these critical operations (Richard de Neufville and Odoni, 2013).

Given the complexity and diversity of activities in both landside and airside areas, these zones are potential targets for acts of unlawful interference. Employees working in these areas must be highly aware of the specific risks associated with each zone to effectively mitigate threats. For instance, landside personnel need to focus on identifying suspicious activities in public spaces, while airside staff must be vigilant about operational safety and security risks around aircraft and restricted areas.

Proactive employee training and awareness programs are essential to maintaining the safety and security of airport infrastructure. By equipping personnel with the knowledge and skills to recognize and respond to potential threats, airports can significantly reduce risks and enhance resilience against unlawful interference. This approach not only strengthens operational safety but also ensures a secure environment for passengers and staff alike.

Unlawful Interference Dimensions

Unlawful interference in civil airports can manifest in various forms, including airport attacks, bomb threats, and even cybersecurity breaches (Alketbi and Sipos, 2024). To understand and address these threats effectively, it is important to identify the primary dimensions that are often targeted. Four key areas of unlawful interference have been identified: attacks on passengers, attacks on airport infrastructure, false and misleading communication, and cyberattacks. Each of these areas represents a critical vulnerability within the civil aviation ecosystem, requiring comprehensive strategies and heightened awareness among airport personnel to mitigate risks and enhance security measures.

Attack on Passengers

Passenger attacks are critical threats to civil aviation, occurring both onboard aircraft and within airport infrastructure. These incidents have significant economic, political, and social impacts, often creating public fear and undermining passenger trust. Understanding the types of attacks and implementing measures to mitigate them is crucial for ensuring safety and security. Employee awareness and preparedness are essential for identifying and responding to these threats effectively. First, aircraft hijacking represents one of the most alarming threats to civil aviation. This involves the unlawful seizure of an aircraft, typically to redirect its destination or use it as a weapon. Notable examples include the 9/11 attacks, where hijacked planes were weaponized to target U.S. landmarks. Other incidents, such as parachute cash heists, highlight hijackings driven by financial motives. Terrorism, political agendas, and psychological factors are common motivations. Employee vigilance and crisis management training are vital in detecting suspicious behaviors and minimizing risks (Lowe, 2014).

Second, bomb threats onboard aircraft pose severe risks due to the potential catastrophic impact of improvised explosive devices (IEDs). These devices can be concealed in luggage or on passengers, as seen in the Mogadishu incident, which resulted in significant destruction. To mitigate such threats, employees must be equipped with advanced screening techniques and trained to recognize behavioral cues that indicate potential danger (Karoly, 2017).

Third, missile attacks are among the most devastating forms of interference with passenger aircraft, often leaving no chance of survival. The downing of Malaysian Airlines flight MH17 underscores the need for geopolitical risk assessments and proactive coordination with air traffic authorities to avoid high-risk areas (Kellman, 2014).

Fourth, robbery onboard aircraft may not pose a direct physical threat but can result in considerable financial and emotional distress for passengers. Theft of personal belongings during flights highlights the importance of employee attentiveness to cabin activities and swift responses to suspicious behavior (Rory, 2007).

Fifth, firearm shootings in airports exploit the public access to landside areas, targeting crowded spaces to inflict maximum harm. Although less frequent, these incidents—such as attacks on airport terminals emphasize the importance of stringent firearm regulations, robust security protocols, and employee readiness for emergencies (Stewart, 2014).

Sixth, bombings within airports, targeting high-density areas, aim to cause mass casualties and widespread disruption. Incidents like the Glasgow Airport bombing attempt demonstrate the necessity for advanced explosive detection systems and vigilant security personnel to prevent such attacks (Breen, 2013). Finally, robbery at airports, ranging from petty theft to organized crime, remains a persistent issue. Effective surveillance systems, close monitoring of baggage claim areas, and timely intervention by employees are critical in reducing such incidents (Kempen, 2017). By systematically addressing these threats through employee training, technological advancements, and coordinated security measures, civil aviation can enhance safety and restore passenger confidence.

Table 2.2
Types of Passenger Attacks

Type of Attack	Description	Examples	Employee Role
Aircraft Hijacking	Unlawful seizure of aircraft for redirection or weaponization.	9/11 attacks, parachute hijacking.	Detect suspicious behavior, follow protocols, communicate effectively with authorities.
Bomb Threats	Use of IEDs onboard aircraft to cause destruction.	Mogadishu explosion (2017).	Conduct thorough screenings, identify suspicious behavior, and respond swiftly to threats.
Missile Attacks	Shooting aircraft with missiles, causing catastrophic damage.	Malaysian Airlines MH17 (2014).	Collaborate on geopolitical risk assessments and ensure coordination with air traffic authorities.
Theft and Robbery	Stealing valuables onboard aircraft.	Parachute heist, onboard thefts.	Monitor passenger behavior, secure valuables, and prevent theft during flights.
Shooting with Firearms	Using firearms in landside areas of airports.	Various global airport shootings.	Monitor public areas, respond to emergencies, and enforce firearm security protocols.
Airport Bombings	Concealing and detonating explosives in crowded airport areas.	Glasgow bombing attempt (2007).	Enhance detection capabilities, train employees in bomb threat protocols, and implement vigilance.
Robbery at Airports	Theft of passengers' belongings in airports, including baggage claim areas.	Global incidents of theft at airports.	Improve surveillance, assist passengers in reporting theft, and secure baggage claim processes.

Attack on Airport Infrastructure

The primary distinction between attacks on passengers at airports and attacks on airport infrastructure lies in the intent and target. Attacks on passengers are primarily aimed at inflicting harm on individuals, often to spread fear or achieve political, religious, or ideological

goals. In contrast, attacks on airport infrastructure are designed to cause significant damage to airport facilities, rendering them inoperable. Such attacks often occur during conflicts or wars, where civil airport runways are targeted to disrupt operations, especially if the facilities are suspected of being used for military purposes. Additionally, these attacks may aim to control or disable navigation systems, halting operations entirely (Siadkowski, 2014; Robert, 2006). According to Stewart (2014), attacks on airport infrastructure are highly hazardous due to the critical role these facilities play in aviation operations. Key targets can include parking areas, curbsides, passenger terminals, concourses, navigation systems, and runways. These acts of destruction, often referred to as sabotage, are frequently driven by political or military motives. By damaging infrastructure, attackers aim to disrupt airport operations on a large scale, causing economic, logistical, and security challenges.

False and Misleading Information / Communication

Communication serves as the backbone of the aviation industry, ensuring the seamless exchange of critical information through various means such as telephones, emails, announcements, and radio messages (Samaras et al., 2019). In civil airports, communication tools are extensively utilized to coordinate operations, maintain safety, and ensure efficiency. However, there are instances where misleading or erroneous communication is deliberately used to jeopardize the safety and security of passengers, airport infrastructure, or aircraft, both on the ground and in the air. Such acts are classified as unlawful interference in civil aviation (Siadkowski, 2014).

False or misleading communication can manifest in numerous ways. According to Sampigethaya (2014), any deceptive or erroneous message within the airport network, whether intentional or accidental, is considered false communication and can severely impact airport security. For instance, interrupting communication within an aircraft cabin can disrupt operations or alter the flight's direction. Similarly, false messages sent to key airport personnel, such as weather updates or operational commands, can result in delayed or canceled flights, compromising safety and efficiency.

Another example of false communication involves tampering with aircraft network systems by introducing viruses. Such acts can disrupt flight schedules, delay take-offs, and complicate operations, creating widespread confusion (Samaras et al., 2019). Additionally, incorrect information provided to ground control units, especially air traffic control towers responsible for slot allocation, can lead to significant issues. When flights miss their designated slots due to false communication, they risk losing landing opportunities, which can further disrupt airport operations and schedules (Sampigethaya, 2014).

In more severe cases, false communication can involve the use of jamming devices. These devices interfere with communication channels, causing confusion for both the sender and receiver of critical messages. This can lead to a breakdown in coordination, heightening risks to safety and security (Samaras et al., 2019).

Given the central role of communication in aviation, safeguarding communication channels from false or misleading information is essential. Robust protocols, advanced technologies, and continuous employee training are necessary to identify and mitigate such threats, ensuring the safety, efficiency, and reliability of civil aviation operations.

Economic Impacts of Unlawful Interference

Economy is the mainstream of any nation; it acts as a chief over other elements. If we took any example of a country that is politically stable with good security principles and sound social environment, it will not be blossoming or flourishing without dynamic and superb economy. Before discussing economic impact, the researcher should discuss the economic purposes of the attack (Niccolo, et. al., 2018). According to (Uzulmez,2016) when terrorists would like to attack a certain airport, they would like to destroy or harm that economy, especially if the country's GDP is relying for a great extent on tourism, as airports are the super gate to any country. On the other hand, sometimes the attack might be since a certain country especially from developing countries, would like to be developed, and a third party may refuse this fact, so that the best way to create a decline on developments' progress is attacking its' airport.

Regarding economic impacts, it is no doubt that the effect of acts of unlawful interference on economy will be tremendous. There will be major consequences for the economy and financial status of the country. The effect will be on both microeconomics and macroeconomics (Niccolo, et. al., 2018). For instance, ticket fares return and service tax per passenger and over all benefits of tourist or business passengers will be knocked out as tourists' confidence rate about that country and its' airline will decrease dramatically (Chen, 2017). Moreover, as mentioned earlier, the effect will not only hit the gross domestic product (GDP), but also unemployment rate would be increased due to job losses as attacks on airports might be major and destroy the full tourism infrastructure. Additionally, prices, currency rates and taxes might be volatile due to negative impact not only tourism, but also on all fields of businesses as most of the countries depend on foreign investors to generate a continuous pump of cash flow (Chen, 2017).

Fly Delays and Cancellations

The cost of a delay per minute is 7,420$. (Daniel A, 2020). When acts of unlawful interference occur, it is normal to expect that flight will be delayed or canceled due to the security procedures and the damage fixing proses (Daniel A, 2020). This delay dose not only effect the airline but also can disrupt other flight scandals, leading to negative impacts of passengers' experience, and can create a ripple effect throughout the entire aviation network, leading to further interference on the airport operations and the economy (Daniel A, 2020).

Airport and Aircraft Repairs

The cost of an A320 aircraft ranges from 77.4 million to 129.5 million $ (Tseko, 2020). The damaged aircraft contribute to the economic risks as they require time, efforts and financial resources to be amended (Tseko, 2020).

Tourism

Unlawful interferences in aviation, such as terrorism, hijackings, cyber-attacks, and sabotage, have profound effects on the tourism sector (Anghuwo, Imanuel and Nangolo, 2024). These incidents create safety concerns, disrupt travel operations, and lead to significant financial losses for airlines, airports, and tourism-related businesses. When aviation security is compromised, travelers become hesitant to visit certain destinations, resulting in a decline in tourist arrivals (Bell, 2022). Governments often issue travel advisories, further discouraging visitors and affecting the economy of tourism-dependent countries. Airlines face increased

operational costs due to heightened security measures, flight cancellations, and rerouting expenses, while hotels, tour operators, and local businesses suffer from reduced bookings and revenue losses. It is vital, therefore, that stringent measures are taken to counter acts of unlawful interference with civil aviation. With unlawful acts, the actual number of casualties is less significant than the threat that everybody who uses air transport could become this (Kazda and Caves, 2010).

Acts of unlawful interferences on aviation effects the tourism sector negatively, as truism depend on transportation to bring visitors, and transportation needs visitors to generate demand depend on transportation and the link between aviation and tourism are being more recognized (Forsyth, 2016). Moreover, tourism is one of the top economic sectors worldwide (Hsu, 2023). However, this industry is always exposure to several risks, particularly unlawful attacks (Florido-Benítez, 2024). Therefore, the reader believes that acts of unlawful interference on civil airports can damage the economy by damaging tourism.

Stocks and Investments

Stocks can indicate the future of the economy (Francesco l, Antonino f, said e, 2011). Attacks on airports effects not only the Stocks of an airline negatively but cause substantial disruptions to essential transportation hubs, resulting in financial losses for the impacted countries (Chen, 2017). The suspension or rerouting of flight operations results in lower income for airlines, airports, and related industries, so negatively impacting the aviation industry, which is a major contributor to economic growth. Furthermore, the ambiguity these initiatives produce fosters an atmosphere of fear that has an immediate effect on investor confidence (Chen, 2017). Investors' reactions to the elevated geopolitical risk frequently result in stock value losses for businesses located in and around damaged airports. In addition, if air travel is disrupted, it can harm other sectors of the economy by impeding the flow of people, products, and services. In general, illegal actions at civil airports have effects that go beyond immediate physical harm, affecting long-term economic stability and investor confidence (Chen, 2017).

Managerial Security Procedures

Managerial security procedures are fundamental to safeguarding civil airports from acts of unlawful interference. Śliwińska (2019) emphasizes the importance of ensuring public security in border areas, where all threatening practices must be closely monitored, and immediate action taken when necessary. Sky marshals on board aircraft must remain vigilant, ready to respond to potential threats, and must maintain effective communication with airport security personnel and local regulatory authorities. Comprehensive reconnaissance of hazards and threats is also critical and can be supported by police officers whose responsibilities include maintaining safety and security across all airport zones and controlling crowd behavior to prevent misuse of uncontrolled areas.

Another vital aspect of managerial security involves countering cyber-attacks targeting airport network systems. These attacks, which can involve the introduction of viruses to compromise passenger data or security protocols, require robust systems to protect critical infrastructure. Unauthorized access to restricted areas must be managed with strict enforcement, including warnings and investigations as necessary. Special attention must also

be given to VIP passengers, who are at a higher risk of being targeted, ensuring their safety through careful escort procedures (Paul et al., 2013).

Governments also play a pivotal role in supporting managerial security measures. Ivančík and Nečas (2020) propose actions such as freezing or confiscating funds linked to terrorist organizations, detaining or deporting individuals suspected of terrorism, and prohibiting asylum for such individuals. Enhanced border and document control systems, including biometric identification and tracking of lost or stolen passports, further bolster airport security. These measures ensure that national and foreign residents are closely monitored to prevent potential threats (Śliwińska, 2019).

The coordination and collaboration of all stakeholders are essential for the successful implementation of these procedures. Check-in agents, cargo acceptance teams, security personnel, and ground staff must work together under the guidance of a duty manager to ensure seamless operations. Effective use of security tools such as CCTV systems, passenger profiling, and advanced screening equipment further enhances the airport's defense against unlawful interference. By integrating managerial, operational, and governmental measures, airports can achieve a high level of preparedness and resilience, safeguarding the aviation industry from evolving threats.

Underpinning Theory

Theoretical frameworks such as Protection Motivation Theory (PMT) and Routine Activity Theory (RAT) offer valuable lenses to understand and enhance awareness of unlawful interference in the UAE's airport sector, particularly regarding attacks on passengers, airport vulnerabilities, and the dissemination of false information. Protection Motivation Theory (PMT), developed by Rogers (1975), is a psychological framework that explains how individuals assess and respond to perceived threats. The theory suggests that people are motivated to protect themselves from threats based on their evaluation of the severity of the threat, their perceived vulnerability to it, their self-efficacy (belief in their ability to take protective actions), and the effectiveness and costs associated with the recommended protective behavior. In the context of airport security, PMT can explain how individuals—such as airport staff or passengers—evaluate the risks posed by unlawful interference and whether they engage in protective behaviors to mitigate these risks.

Routine Activity Theory (RAT), developed by Cohen and Felson (1979), focuses on the situational and environmental factors that contribute to the occurrence of crime. The theory posits that criminal acts are more likely to occur when three elements converge: a motivated offender, a suitable target, and the absence of a capable guardian. RAT emphasizes the importance of routine activities and everyday patterns of life in shaping criminal opportunities. In the context of airports, RAT can help explain how the structure of airport operations, the presence or absence of effective security measures, and the vulnerabilities in routine activities might create opportunities for unlawful interference, such as attacks on passengers, damage to infrastructure, or the spread of false information.

These variables significantly influence readiness to mitigate the effects of such interference on critical sectors, including economic stability, tourism, airport and aircraft maintenance, and infrastructure resilience. PMT provides a structured approach to understanding how

awareness of passenger attacks can drive preventive behaviors. The theory's threat appraisal component emphasizes perceived severity and vulnerability, which are critical to shaping awareness among airport authorities, employees, and passengers. For instance, the perception of severe consequences of passenger-targeted attacks—such as economic losses or harm to public safety—can motivate airport personnel to implement enhanced security measures. Research by Rogers (1983) underscores how perceived vulnerability to such threats compels individuals to adopt protective actions, such as heightened vigilance and compliance with safety protocols. Simultaneously, RAT explains how situational factors in the airport environment contribute to the risk of passenger-targeted attacks. The presence of a motivated offender, suitable targets (e.g., large crowds of travelers), and the absence of capable guardians (e.g., insufficient security personnel or monitoring) create opportunities for unlawful interference (Cohen & Felson, 2003). For example, routine activities such as baggage screening or ticketing can become vulnerabilities if security measures are inconsistently applied. Addressing these risks requires not only awareness but also systemic changes in operational routines and resource allocation (Hutchings & Hayes, 2009).

Airport infrastructure represents a critical point of vulnerability to unlawful interference. PMT highlights how awareness of these vulnerabilities—through perceived severity and response efficacy can drive readiness to mitigate risks. For example, perceived severity of infrastructural disruptions, such as terminal closures or delays due to security breaches, may encourage investments in preventive technologies like biometric access controls and AI-driven threat detection systems (Salehi, 2021). Similarly, response efficacy can be enhanced by demonstrating the effectiveness of these technologies in mitigating risks, thereby increasing organizational confidence in their implementation (Briggs et al., 2017). RAT complements this by identifying specific vulnerabilities within routine airport operations.

These include the predictable scheduling of flights, the centralized processing of passengers, and the use of digital systems that may lack robust cybersecurity measures (Choi & Young, 2021). The absence of capable guardians, such as inadequate IT security protocols or a lack of trained cybersecurity personnel, exacerbates these vulnerabilities. Cohen and Felson's (2003) framework emphasize that addressing these gaps requires both situational awareness and operational changes, such as increasing patrols or deploying redundant systems to safeguard critical infrastructure. The interplay between PMT and RAT helps to contextualize how awareness of airport vulnerabilities impacts broader outcomes. For example, effective threat appraisal and coping appraisal can reduce the likelihood of operational disruptions that affect aircraft maintenance, repairs, and passenger flows, safeguarding economic activity and tourism. Additionally, investments in infrastructure resilience—such as redundant power supplies and secure data networks mitigate the economic and reputational costs of unlawful interference.

The dissemination of false information poses a unique challenge to the readiness of airport authorities and passengers to mitigate risks. PMT explains how perceived severity and vulnerability to misinformation can shape awareness and protective behaviors. For example, misinformation about security threats can lead to panic or misinformed responses, disrupting airport operations and eroding passenger trust. Self-efficacy, a key component of coping appraisal, can empower individuals and organizations to critically assess information and

respond effectively, such as by relying on verified sources or implementing misinformation detection systems (Li et al., 2016).

RAT, on the other hand, sheds light on the situational dynamics that facilitate the spread of false information. Airports, as highly interconnected and fast-paced environments, are particularly susceptible to the rapid dissemination of misinformation through social media and other digital platforms. The absence of a capable guardian, such as real-time monitoring of communication channels or public information officers, creates opportunities for motivated offenders to exploit these vulnerabilities (Hutchings & Hayes, 2009). Integrating PMT and RAT can enhance readiness to address the economic and operational impacts of misinformation. For example, routine information verification processes and employee training can address the absence of capable guardians, while awareness campaigns that emphasize the severity of misinformation's consequences encourage vigilance among stakeholders. This dual approach minimizes disruptions to tourism, infrastructure, and economic stability caused by mi Both Protection Motivation Theory (PMT) and Routine Activity Theory (RAT) offer valuable frameworks for understanding unlawful interference in airport operations. However, RAT is particularly suitable for analyzing unlawful interference at airports, as it focuses on situational factors and environmental conditions that increase the likelihood of criminal activities, making it highly relevant to the real-world scenarios at airports. RAT, developed by Cohen and Felson (1979), posits that criminal acts, including unlawful interference, occur when three key elements converge: a motivated offender, a suitable target, and the absence of a capable guardian. This emphasis on situational and environmental factors is crucial in the context of airport security, where the complex and dynamic nature of operations creates various potential vulnerabilities.

RAT's application to the airport setting highlights how factors such as crowded terminals, reduced security during certain times, or gaps in surveillance can create opportunities for unlawful interference. For example, at certain times, airports may have areas with less oversight or fewer security personnel, which increases the risk of attacks on passengers or damage to infrastructure. Additionally, RAT explains how weak points in routine operations, such as under-resourced areas or high passenger traffic during peak hours, can make the airport a suitable target for motivated offenders. The absence of capable guardians—such as insufficient security staff, ineffective surveillance, or gaps in communication systems—further exacerbates this risk.

The Justification of Using Routine Activity Theory (RAT)

The decision to select RAT over PMT is based on its structural and environmental focus, which is more appropriate for addressing the dynamic, everyday routines of airport operations. While PMT centers on individual decision-making and the psychological aspects of threat perception, RAT examines how environmental and situational factors contribute to opportunities for criminal acts. In airports, this includes how routine activities, such as passenger movement or aircraft handling, can inadvertently create openings for unlawful interference. Additionally, RAT's focus on the convergence of motivated offenders, suitable targets, and the absence of capable guardians provides a more practical approach to addressing security vulnerabilities in airport settings. Furthermore, applying RAT to attacks on passengers, airport infrastructure, and the spread of false information shows how these factors interact to increase risk. False information can disrupt routine operations by

undermining public confidence in airport security, creating panic, or even drawing resources away from actual security concerns. The spread of misinformation can make airports appear less capable of managing risks, further diminishing their ability to respond effectively to unlawful interference. Therefore, understanding these dynamics through RAT provides clearer insight into how routine airport operations and security measures may unintentionally create opportunities for unlawful acts.

However, it is crucial to recognize that each airport has its own protection culture and operational practices, which may influence how routine activities and security measures contribute to vulnerabilities. Therefore, it is important to validate the employees' awareness of unlawful interference at the airport. Understanding the actual practices and effectiveness of security measures, as well as the level of awareness among airport staff, is essential for developing tailored strategies to mitigate the impact of unlawful interference. This will help improve readiness in addressing economic factors, tourism, infrastructure, and aircraft maintenance, ultimately strengthening airport security and reducing vulnerabilities.

Hypotheses Development

Awareness of Passenger Attacks

Employee awareness plays a critical role in mitigating the negative economic impacts of passenger attacks in civil aviation. Employees who are knowledgeable about different types of attacks, such as hijackings, bomb threats, missile attacks, and robberies, can effectively prevent security breaches and minimize their consequences (Avc & Civelek, 2017; Śliwińska, 2019). Awareness programs that focus on safety protocols, reporting procedures, and emergency response preparedness ensure that employees are equipped to handle potential threats. This proactive approach not only strengthens security measures but also helps reduce the economic repercussions of such incidents (Heng et al., 2015).

Effective employee awareness has direct implications for controlling the economic effects of flight delays and cancellations. Clear communication with passengers during disruptions, coupled with efficient resource management and coordinated departmental efforts, minimizes financial losses and preserves passenger satisfaction (Stewart, 2013). Moreover, adherence to safety protocols and timely identification of security threats prevent unplanned maintenance and repairs, reducing costs and operational downtime (Breen, 2013). Employees trained to manage disruptions can also optimize schedules and avoid unnecessary expenditures.

Tourism, a vital economic contributor, is equally impacted by passenger attacks. Prompt reporting of threats by employees ensures a safe travel environment, which boosts traveler confidence and attracts more tourists (Kempen, 2017). Coordinated operations and the prevention of unnecessary disruptions improve the overall tourist experience, encouraging repeat visits and maintaining steady tourism flows (Elzawi & Eaton, 2010). Similarly, in the context of stock performance and investment, early detection of security threats by employees maintains investor confidence, reduces costly delays, and ensures smooth financial operations (Kellman, 2014). By addressing false information and responding quickly to disruptions, employees contribute to the stability and profitability of aviation-related investments.

Employee readiness and awareness are central to mitigating the broad economic impacts of passenger attacks. Whether through safeguarding passenger trust, minimizing disruptions, or supporting operational efficiency, a well-trained workforce is an indispensable asset in maintaining the resilience and economic viability of the aviation industry (Hamisi, 2018).

Employee awareness plays a crucial role in mitigating passenger attacks and ensuring the economic stability of airports. According to (Bell, 2022), a lack of proper employee training and awareness in handling disruptive passenger behavior contributes to recurring incidents that disrupt airport operations and increase operational costs. The study highlights that when employees, particularly frontline staff, feel unsupported by management and are not given clear protocols to enforce disciplinary measures against unruly passengers, it creates an environment where passengers perceive that disruptive actions carry minimal consequences. This, in turn, encourages repeated misconduct, leading to flight delays, legal liabilities, and increased security expenses. Moreover, ineffective handling of such incidents can deter travelers, impacting passenger confidence and reducing revenue from airline ticket sales, airport concessions, and related services. Implementing a robust Safety Management System (SMS) that prioritizes employee training, de-escalation techniques, and a strong safety culture can significantly reduce the frequency of such incidents, ensuring smoother airport operations and sustained economic performance (Bell, 2022).

Therefore, this research hypothesizes that:
H1: Employees' awareness of passenger attacks has a significant positive relationship with their readiness capabilities to mitigate the economic effects of flight delays and cancellations
H2: Employees' awareness of passenger attacks has a significant positive impact on their readiness capabilities to mitigate tourism disruptions
H3: Employees' awareness of passenger attacks has a significant positive impact on their readiness capabilities to mitigate the effects on stocks and investments
H4: Employees' awareness of passenger attacks has a significant positive impact on their readiness capabilities to mitigate the effects on maintenance and repairs

Employee Awareness in Airport Infrastructure Attacks
Awareness of airport security threats among employees plays a vital role in mitigating the economic impacts of attacks on airport infrastructure. Employees who are informed about potential threats, such as bomb threats or cyber-attacks, contribute significantly to early detection and prevention, which directly reduces operational disruptions (Piekert et al., 2024). A clear understanding of the steps taken to secure facilities enhances employees' confidence in implementing safety measures and reporting unusual activities, which strengthens the overall security framework of the airport (Florido-Benítez, 2024).

This proactive employee awareness supports the mitigation of economic effects in multiple areas. For instance, during flight delays and cancellations, employees who are prepared to act can ensure efficient communication with passengers, minimizing confusion and maintaining customer satisfaction (Skorupski and Uchroński, 2018). This reduces revenue losses associated with delays while also helping to manage resources effectively. Prompt departmental coordination, supported by well-trained staff, further minimizes the financial setbacks caused by extended disruptions (Piekert et al., 2024).

Similarly, awareness and preparedness among employees have a direct impact on airport and aircraft maintenance and repairs. Early reporting of security threats helps avoid costly damage and unnecessary repairs. By following established safety protocols and responding quickly to disruptions, employees optimize maintenance schedules, reduce downtime, and minimize associated costs. Their ability to identify and address false information also prevents unnecessary maintenance actions, ensuring efficient resource utilization.

Tourism, a key economic driver, also benefits from employee awareness of airport threats. Employees who report security risks early help maintain a safe environment, attracting tourists and preventing disruptions that could deter travel. Coordinated operations ensure smooth airport functionality, which enhances the overall travel experience and encourages repeat visits (Piekert et al., 2024). Additionally, by addressing misinformation and acting swiftly during emergencies, employees maintain a steady flow of tourism and preserve the airport's reputation. Therefore, this research hypothesizes that:

H5: Employees' awareness of airport infrastructure attacks has a significant positive relationship with their readiness capabilities to mitigate the economic effects of flight delays and cancellations
H6: Employees' awareness of airport infrastructure attacks has a significant positive impact on their readiness capabilities to mitigate tourism disruptions
H7: Employees' awareness of airport infrastructure attacks has a significant positive impact on their readiness capabilities to mitigate the effects on stocks and investments
H8: Employees' awareness of airport infrastructure attacks has a significant positive impact on their readiness capabilities to mitigate the effects on maintenance and repairs

Awareness of False Information

Awareness of false information and its impact on communication within the aviation sector is a critical factor in mitigating economic disruptions at airports. Employees who are trained to recognize misleading communications and verify their authenticity play a vital role in maintaining operational efficiency. Misleading information, such as incorrect weather updates or false security alerts, can lead to delayed flights, canceled schedules, and even compromised passenger safety. By identifying and addressing such issues early, employees help prevent confusion and ensure smoother operations.

The ability of employees to handle incidents involving false information has a direct effect on the economic performance of airports. Effective communication with passengers during disruptions minimizes uncertainty, preserving customer trust and satisfaction. Efficient management of resources during flight cancellations or delays further reduces financial losses. Additionally, coordinated departmental efforts, driven by informed employees, help streamline operations and mitigate the cascading costs caused by prolonged disruptions.

In the context of airport and aircraft maintenance, awareness of false information ensures accurate reporting and prevents unnecessary checks or repairs. Employees who understand the protocols for addressing misleading data can avoid operational downtime and costly maintenance errors. Their ability to respond promptly to security threats also enhances the reliability of maintenance schedules, reducing unplanned expenses and ensuring continued service.

Tourism, a key revenue stream for many airports, is also protected by employee vigilance in handling false information. Early identification of security risks helps maintain a safe and seamless travel experience, encouraging repeat visits and attracting more travelers. Coordinated operations and the prevention of misinformation-related disruptions enhance tourist confidence, fostering a steady flow of visitors and preserving the airport's reputation.

Finally, the financial health of airports, including their attractiveness to investors, is closely linked to how well employees handle false information. Detecting security threats early and ensuring smooth operations help stabilize stock performance and strengthen investor trust. Consistent safety practices and quick responses to disruptions not only mitigate economic losses but also boost the airport's financial appeal. Therefore, this research hypotheses that:

H9: Employees' awareness of airport infrastructure attacks has a significant positive relationship with their readiness capabilities to mitigate the economic effects of flight delays and cancellations
H10: Employees' awareness of airport infrastructure attacks has a significant positive impact on their readiness capabilities to mitigate tourism disruptions
H11: Employees' awareness of airport infrastructure attacks has a significant positive impact on their readiness capabilities to mitigate the effects on stocks and investments
H12: Employees' awareness of airport infrastructure attacks has a significant positive impact on their readiness capabilities to mitigate the effects on maintenance and repairs

Moderate Effect of Managerial Security Procedures

Managerial security procedures play a critical role in ensuring the safety, efficiency, and resilience of civil aviation. Airports, as complex and dynamic environments, require coordinated efforts to mitigate risks and safeguard operations against an array of potential threats, including unlawful interference, cyber-attacks, and physical sabotage. Managerial security encompasses the strategic oversight, policies, and protocols that align the efforts of various stakeholders, including employees, passengers, airlines, security personnel, and regulatory authorities, to maintain operational continuity and mitigate economic and reputational losses. The moderating effect of managerial security procedures on the relationship between employees' awareness and their readiness capabilities to mitigate economic and operational impacts is pivotal to ensuring a secure and resilient airport environment. Managerial procedures, including robust protocols, effective communication, and advanced monitoring mechanisms, enhance the impact of employees' awareness in addressing threats (Śliwińska, 2019; Ivančík & Nečas, 2020). Below, new hypotheses are summarized under each sub-discussion.

Employees' awareness of passenger and airport infrastructure attacks significantly influences their readiness to mitigate the economic effects of flight delays and cancellations. Managerial security procedures, by ensuring clear protocols and efficient resource allocation, amplify this relationship. Recent research highlights that managerial oversight facilitates operational efficiency during disruptions, reducing financial losses and maintaining customer satisfaction (Stewart, 2019; Ogonowski et al., 2020). Therefore, this research hypothesizes that managerial security procedures moderate the relationship between employees' awareness of attacks and their readiness capabilities to mitigate the economic impacts of flight delays and cancellations.

H13: Managerial security procedures moderate the relationship between Employees' awareness of passenger attacks and readiness capabilities to mitigate the economic effects of flight delays and cancellations

H14: Managerial security procedures moderate the relationship between employees' awareness of passenger attacks and readiness capabilities to mitigate tourism disruptions.

H15: Managerial security procedures moderate the relationship between employees' awareness of passenger attacks and readiness capabilities to mitigate the effects on stocks and investments.

H16: Managerial security procedures moderate the relationship between employees' awareness of passenger attacks and readiness capabilities to mitigate the effects on maintenance and repairs.

The ability of employees to address tourism disruptions caused by airport infrastructure attacks is enhanced by managerial security procedures. These procedures provide structured guidelines for managing crises and ensuring seamless operations in tourist-sensitive areas. Effective managerial interventions enable employees to maintain traveler confidence and support tourism recovery (Paul et al., 2013; Tan, 2016). Therefore, this research hypothesizes that managerial security procedures moderate the relationship between employees' awareness of attacks and their readiness capabilities to mitigate tourism disruptions.

H17: Managerial security procedures moderate the relationship between employees' awareness of airport infrastructure attacks and readiness capabilities to mitigate the economic effects of flight delays and cancellations

H18: Managerial security procedures moderate the relationship between employees' awareness of airport infrastructure attacks and readiness capabilities to mitigate tourism disruptions.

H19: Managerial security procedures moderate the relationship between employees' awareness of airport infrastructure attacks and readiness capabilities to mitigate the effects on stocks and investments.

H20: Managerial security procedures moderate the relationship between employees' awareness of airport infrastructure attacks and readiness capabilities to mitigate the effects on maintenance and repairs.

Employees' awareness of security threats contributes significantly to maintaining investor confidence and stabilizing financial performance. Managerial security procedures enhance this relationship by fostering clear communication and timely responses to operational disruptions. Studies suggest that managerial practices, such as effective reporting and risk management, are crucial for protecting stock performance and attracting investments (Ivančík & Nečas, 2020; Śliwińska, 2019). Therefore, this research hypothesizes that managerial security procedures moderate the relationship between employees' awareness of attacks and their readiness capabilities to mitigate impacts on stocks and investments.

H21: Managerial security procedures moderate the relationship between Employees' awareness of False information/communication and readiness capabilities to mitigate the Stocks and Investments

H22: Managerial security procedures moderate the relationship between employees' awareness of False information/communication and readiness capabilities to mitigate tourism disruptions.
H23: Managerial security procedures moderate the relationship between employees' awareness of False information/communication and readiness capabilities to mitigate the effects on stocks and investments.
H24: Managerial security procedures moderate the relationship between employees' awareness of False information/communication and readiness capabilities to mitigate the effects on maintenance and repairs.

Research Framework

The proposed research framework integrates employee awareness, managerial security procedures, and economic impacts within the civil aviation sector, focusing on mitigating passenger and airport infrastructure attack effects and false information communication. The framework is structured as follows:

Awareness of Passenger Attacks

Employee awareness of passenger attacks, such as hijackings, bomb threats, missile attacks, and robberies, directly influences their readiness to mitigate economic disruptions. This includes minimizing flight delays, cancellations, and maintenance costs, preserving tourism flows, and stabilizing stock and investment performance.

H1: Employees' awareness of passenger attacks has a significant positive relationship with their readiness capabilities to mitigate the economic effects of flight delays and cancellations.
H2: Employees' awareness of passenger attacks has a significant positive impact on their readiness capabilities to mitigate tourism disruptions.
H3: Employees' awareness of passenger attacks has a significant positive impact on their readiness capabilities to mitigate the effects on stocks and investments.
H4: Employees' awareness of passenger attacks has a significant positive impact on their readiness capabilities to mitigate the effects on maintenance and repairs.

Awareness of Airport Infrastructure Attacks

Awareness of threats targeting airport infrastructure, such as cyber-attacks and bomb threats, enhances employees' readiness to mitigate economic effects through effective threat detection, coordinated responses, and operational continuity.

H5: Employees' awareness of airport infrastructure attacks has a significant positive relationship with their readiness capabilities to mitigate the economic effects of flight delays and cancellations.
H6: Employees' awareness of airport infrastructure attacks has a significant positive impact on their readiness capabilities to mitigate tourism disruptions.
H7: Employees' awareness of airport infrastructure attacks has a significant positive impact on their readiness capabilities to mitigate the effects on stocks and investments.
H8: Employees' awareness of airport infrastructure attacks has a significant positive impact on their readiness capabilities to mitigate the effects on maintenance and repairs.

Awareness of False Information Communication

Employee vigilance in identifying and addressing false information ensures operational efficiency and reduces economic losses across multiple areas, including maintenance, tourism, and financial stability.

H9: Employees' awareness of false information communication has a significant positive relationship with their readiness capabilities to mitigate the economic effects of flight delays and cancellations.

H10: Employees' awareness of false information communication has a significant positive impact on their readiness capabilities to mitigate tourism disruptions.

H11: Employees' awareness of false information communication has a significant positive impact on their readiness capabilities to mitigate the effects on stocks and investments.

H12: Employees' awareness of false information communication has a significant positive impact on their readiness capabilities to mitigate the effects on maintenance and repairs.

Moderating Effect of Managerial Security Procedures

Managerial security procedures, encompassing oversight, training, and communication protocols, moderate the relationship between employee awareness and readiness capabilities. These procedures amplify the effectiveness of awareness in addressing economic impacts.

H13: Managerial security procedures moderate the relationship between employees' awareness of passenger attacks and readiness capabilities to mitigate the economic effects of flight delays and cancellations.

H14: Managerial security procedures moderate the relationship between employees' awareness of passenger attacks and readiness capabilities to mitigate tourism disruptions.

H15: Managerial security procedures moderate the relationship between employees' awareness of passenger attacks and readiness capabilities to mitigate the effects on stocks and investments.

H16: Managerial security procedures moderate the relationship between employees' awareness of passenger attacks and readiness capabilities to mitigate the effects on maintenance and repairs.

Airport Infrastructure Attacks

H17: Managerial security procedures moderate the relationship between employees' awareness of airport infrastructure attacks and readiness capabilities to mitigate the economic effects of flight delays and cancellations.

H18: Managerial security procedures moderate the relationship between employees' awareness of airport infrastructure attacks and readiness capabilities to mitigate tourism disruptions.

H19: Managerial security procedures moderate the relationship between employees' awareness of airport infrastructure attacks and readiness capabilities to mitigate the effects on stocks and investments.

H20: Managerial security procedures moderate the relationship between employees' awareness of airport infrastructure attacks and readiness capabilities to mitigate the effects on maintenance and repairs.

False Information Communication

H21: Managerial security procedures moderate the relationship between employees' awareness of false information communication and readiness capabilities to mitigate the economic effects of flight delays and cancellations.

H22: Managerial security procedures moderate the relationship between employees' awareness of false information communication and readiness capabilities to mitigate tourism disruptions.

H23: Managerial security procedures moderate the relationship between employees' awareness of false information communication and readiness capabilities to mitigate the effects on stocks and investments.

H24: Managerial security procedures moderate the relationship between employees' awareness of false information communication and readiness capabilities to mitigate the effects on maintenance and repairs.

This research framework integrates these hypotheses to analyze the interplay between employee awareness, managerial security procedures, and economic impacts, providing a holistic understanding of how to enhance the resilience and sustainability of the civil aviation industry.

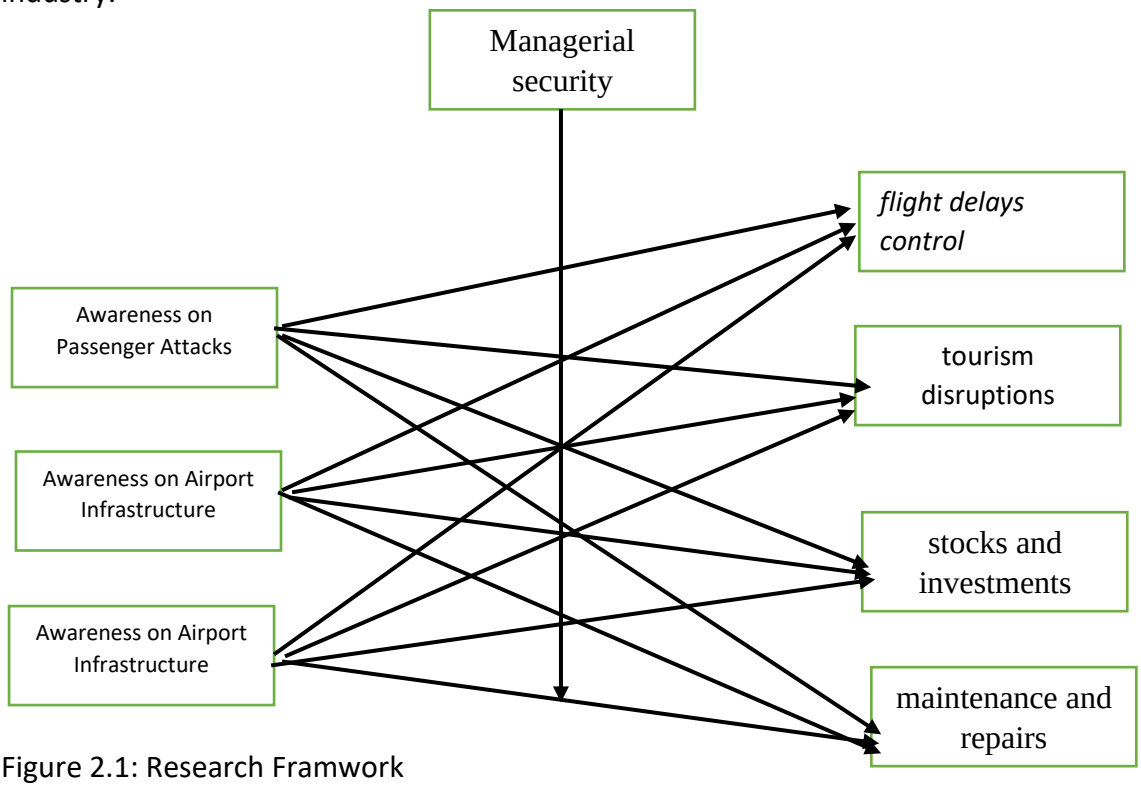

Figure 2.1: Research Framwork

Significance of the Study

This study holds significant importance for both academic research and practical applications in the field of aviation security and economic resilience. By examining the relationship between employee awareness of unlawful interference—specifically attacks on passengers, infrastructure sabotage, and misinformation—and the economic stability of Abu Dhabi

International Airport (AUH), the research provides valuable insights into mitigating risks in critical aviation hubs. The findings contribute to the existing literature by integrating Routine Activity Theory (RAT) to explain how situational factors and employee preparedness influence security outcomes. Furthermore, the study highlights the moderating role of managerial security procedures, offering a structured approach for policymakers and airport authorities to enhance threat detection and response mechanisms. Given AUH's strategic role in global aviation and the UAE's economy, this research underscores the necessity of continuous employee training, robust security protocols, and proactive risk management to safeguard economic stability, tourism, and investor confidence. The implications extend beyond AUH, serving as a model for other international airports facing similar security and economic challenges.

Conclusion

In conclusion, this study emphasizes the critical role of employee awareness in mitigating the economic impacts of unlawful interference at Abu Dhabi International Airport. By analyzing three key dimensions—attacks on passengers, infrastructure sabotage, and misinformation—the research demonstrates that well-trained employees can significantly reduce disruptions in flight operations, maintenance costs, tourism flows, and financial stability. The application of Routine Activity Theory (RAT) reinforces the importance of situational measures, such as capable guardianship and target hardening, in preventing security breaches. Additionally, the moderating effect of managerial security procedures highlights the need for structured policies, clear communication, and coordinated responses to enhance readiness capabilities. The proposed conceptual framework and hypotheses provide a foundation for future empirical studies, while the practical recommendations offer actionable strategies for airport authorities to strengthen security measures. Ultimately, fostering a culture of vigilance, continuous training, and adaptive security policies will not only protect AUH's operational efficiency but also ensure its long-term economic resilience in an increasingly complex global aviation landscape.

References

Abeyratne, R. I. (2024). Treaties Establishing ICAO And IMO – A Comparative Study. *Journal of Air Law and Commerce*, 89(2), pp.297–351.

Alards-Tomalin, D., Ansons, T. L., Reich, T. C., Sakamoto, Y., Davie, R., Leboe-McGowan, J. P., and Leboe-McGowan, L. C. (2014). Airport security measures and their influence on enplanement intentions: Responses from leisure travelers attending a Canadian University. *Journal of Air Transport Management*, 37, pp.60–68.

Alketbi, K., and Sipos, A. (2024). The role of smart technology in airport facilitation and security control (ICAO Annex 9 and 17 requirements). *Journal of Infrastructure, Policy and Development*, 8(8), pp.1–17.

Anghuwo, J. S., Imanuel, P., and Nangolo, S. S. (2024). Anti-unmanned aerial vehicle detection system for airports: aviation and national security perspective. *Journal of Transportation Security*, 17(1), pp.1–17.

ATAG. (2018). Powering global economic growth, employment, trade links, tourism and support for sustainable development through air transport. *Aviation Benefits Beyond Borders*, p.88.

Bell, K. D. A. (2022). An evaluation into the causes of perpetual disruptive passenger behavior. *Journal of Transportation Security*, 15(1–2), pp.1–22.

Buchan, R. (2012). Cyber attacks: Unlawful uses of force or prohibited interventions? *Journal of Conflict and Security Law*, 17(2), pp.212-227.

Burlov, V., Gryzunov, V., Koryakina, A., and Ukraintseva, D. (2022). Management of the Airport Security Process Based on the Conservation Law of the Object's Integrity. *Lecture Notes in Networks and Systems*, 1281–1289 2022.

Calzada, J., and Fageda, X. (2023). Airport dominance, route network design and flight delays. *Transportation Research Part E: Logistics and Transportation Review*, 170, p.103000.

Dimitriou, D., Sartzetaki, M., and Karagkouni, A. (2025). Airport Landside Area Planning: An Activity-Based Methodology for Seasonal Airports. *Transportation Research Procedia*, 82(July 2023), pp.1167–1184.

Florido-Benítez, L. (2024). *The types of hackers and cyberattacks in the aviation industry*, Springer US.

Forsyth, P. (2016). Tourism and Aviation Policy: Exploring the Links. In *Aviation and Tourism: Implications for Leisure Travel*, pp. 1–10.

Gössling, S., and Humpe, A. (2020). The global scale, distribution and growth of aviation: Implications for climate change. *Global Environmental Change*, 65, p.102194.

Hanus, B., and Wu, Y. "Andy," (2016). Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management*.

Hollerer, S., Sauter, T., and Kastner, W. (2022). Risk Assessments Considering Safety, Security, and Their Interdependencies in OT Environments. *ACM International Conference Proceeding Series*, 1–8 2022.

Hsu, H. (2023). "Smart cities and tourism: co-creating experiences, challenges and opportunities." *Information Technology & Tourism*, 25, pp.259–261.

Al Jasmi, M. I. H. M., Mohd Udin, M. binti, and R. A. Siam, M. (2021). Impact of Crisis Management Practices on the Effectiveness of Crisis Management of Drones Threats in Abu Dhabi International Airport. *South Asian Journal of Social Sciences and Humanities*, 2(3), pp.1-17.

Kazda, T., and Caves, B. (2010). Passenger Terminals. In *Airport Design and Operation*, pp. 281-310.

Lee, H. P., Kumar, S., Garg, S., and Lim, K. M. (2022). Assessment of in-cabin noise of wide-body aircrafts. *Applied Acoustics*, 194, p.108809.

El Naggar, H., and Abdelrazik, H. (2024). Assessing community awareness for flood disasters in the UAE through human-centered design. *International Journal of Disaster Risk Reduction*, 107(April), p.104475.

Pham, M., and Xiong, K. (2021). A survey on security attacks and defense techniques for connected and autonomous vehicles. *Computers and Security*, 109, p.102269.

Piekert, F., Schaper, M., Stelkens-Kobsch, T. H., Predescu, A.-V., Günther, Y., and Carstengerdes, N. (2024). Mitigation of operational impacts on airports by early awareness of malicious events impacting linked critical infrastructures. *Journal of the Air Transport Research Society*, 2, p.100011.

Rashad, Fatima, Ali, N.A., Kudus, N., Kamalrudin, M., Akmal, S., and Hakimi, H. (2024). Analyzing Factors of Employee Engagements to Enhance Job Satisfaction among the Employees in United Arab Emirates. , 14(8), pp.1953–1965.

Richard de Neufville, and Odoni, A. R. (2013). *Airport Systems Planning, Design, and Management*, New York Chicago San Francisco.

Skorupski, J., and Uchroński, P., 2018. Management of airport security screening system

effectiveness. *Safety and Reliability - Safe Societies in a Changing World - Proceedings of the 28th International European Safety and Reliability Conference, ESREL 2018*, pp.2931–2938.

Skorupski, J., Uchroński, P., and Łach, A. (2018). A method of hold baggage security screening system throughput analysis with an application for a medium-sized airport. *Transportation Research Part C: Emerging Technologies*, 88(November 2017), pp.52–73.

Sun, X., Wandelt, S., and Zhang, A. (2020). Resilience of cities towards airport disruptions at global scale. *Research in Transportation Business and Management*, 34, p.100452.

Teichmann, F., Boticiu, S.R., and Sergi, B. S. (2023). The evolution of ransomware attacks in light of recent cyber threats. How can geopolitical conflicts influence the cyber climate? *International Cybersecurity Law Review*, 4(3), pp.259-280.

Vadaparthi, V. V. (2017). *Design Analysis of a Narrow Body Medium Range Commercial Aircraft*. San José State University.

Verde, A. (2024). *Competition Dynamics and Market Power: Analysis of the Duopoly Between Airbus and Boeing in the Civil Aircraft Manufacturing Industry*.

Wandelt, S., and Wang, K. (2024). Towards solving the airport ground workforce dilemma: A literature review on hiring, scheduling, retention, and digitalization in the airport industry. *Journal of the Air Transport Research Society*, 2, p.100004.

Yu, D. (2020). Global Aircraft Leasing Industry Characteristics. In *Aircraft Valuation*, pp. 33-95.

ZAG, K., ALS, E.R.I., and INOV, I.D.E. (2021). *D7. 3–Best practices for updating airport security standard and policies*,