RISK ASSESSMENT OF AVIATION SECURITY AND EVALUATION OF AVIATION SECURITY POLICIES

Ramazan Yalcinkaya, B.A.

Thesis Prepared for the Degree of

MASTER OF SCIENCE

UNIVERSITY OF NORTH TEXAS

August 2005

APPROVED:

Eric J. Fritsch, Major Professor, Graduate
Advisor and Chair
Bradley Chilton, Committee Member
D. Kall Loper, Committee Member
Robert W. Taylor, Chair of the Department
of Criminal Justice
David W. Hartman, Dean of the School of
Community Services
Sandra L. Terrell, Dean of the Robert B.
Toulouse School of Graduate Studies

ProQuest Information and Learning Company
300 North Zeeb Road
P.O. Box 1346
Ann Arbor, MI 48106-1346

Yalcinkaya, Ramazan, *Risk Assessment of Aviation Security and Evaluation of Aviation Security Policies*. Master of Science (Criminal Justice), August 2005**,** 112 pp.**,** references, 78 titles.

Comprising many airplanes, airports, aircrew, and employees, aviation industry is a large sector that is very vulnerable to attacks, whether it is from terrorists or criminals. Aviation history is fraught with examples of airport bombings, hijackings, and sabotage terrorist attacks. The most destructive of which is the tragedy of September 11, 2001, the cornerstone of today's aviation security policies. This study uses risk assessment tools to determine the dimensions of danger and threats against the aviation industry and addresses how vulnerable the aviation sector is. After vulnerabilities and threats are examined, possible impacts of attacks against the aviation security are discussed.

This study also explores the pre and post September 11 policies that governments and policy makers develop to reduce risks in aviation sector. In addition, it discusses weaknesses and strengths of these policies which surfaced during the implementations. Finally, this study proposes some recommendations based on vulnerabilities and threats of aviation security.

ACKNOWLEDGMENTS

First of all, I would like to express my sincere thanks to Turkish National Police (TNP) for supporting financially and giving the opportunity of attending this program.

I appreciate to the chair of my committee, Dr. Fritsch, for his supervision, encouragement, and invaluable discussions. I also thanks to Dr. Chilton and Dr. Loper for their time and assistance as a member of my committee. Furthermore, I would like to thank to my English teacher, Tran Chou, for editing this study.

Last but not least, I am grateful to my parents, my wife, Nilgun, and my daughters, Selin and Nilsu, for their patience, encouragement and support.

TABLE OF CONTENTS

Page

Chapter

CHAPTER 1

INTRODUCTION

In an era in which people live a fast-paced life and technological advances occur at a rapid rate, it cannot be denied that aviation is one of the most important industries in the world. It has changed the way we live drastically by carrying millions of people and millions of tons of cargo long distances in a relatively short amount of time. Since aviation began, traveling long distances has been measured by hours instead of days and weeks (Thomas, 2003). People all over the world have used airplanes for leisure, business travel and transportation of goods (Ghobrial & Irvin, 2004). Moreover, airplanes have been considered the showcases and representatives of the nations whose flags they fly (Dempsey, 2003a).

In the United States, which provides 40% of all flights in the world, there are 5,000 airports, 55,000 pilots, 200,000 private airplanes, 475 commercial airport supervisors, and 7,000 air traffic controllers (Szyliowicz, 2004; Thomas, 2003). Every day 2 million passengers travel on 30,000 flights, and 450,000 millions of tons of cargo is transported via planes each year (Thomas, 2003). The quantity of transported goods, business travel, and employed workers for this sector show how important a role it plays in the economy (Ghobrial & Irvin, 2004). In the United States, the aviation sector makes up 6%-7% of the nation's gross domestic product or GDP (Szyliowicz, 2004).

Because of the many vulnerabilities of aviation systems and the harmful impact of attacks on it, the aviation industry has continued to be a preferred target for terrorists and criminals (Garvey, 2002). Almost all plane crashes result in many fatalities and draw maximum media attention, which they can use to further express their ideologies. Terrorist attacks appear in the forms of bombing airports and airplanes, hijacking, sabotaging, and issuing bomb threats. Due to the fact that terrorism involves using violence, many people have suffered greatly from terrorist attacks, and these attacks on the aviation industry always result in catastrophes (Sweet, 2002). In addition to these kinds of attacks, transportation via aviation itself has inherent safety risks even though the number of deaths in plane accidents is less than that for other types of transportation systems when compared annually (Cobb & Primo, 2003). For these reasons, aviation security, which is attributable to techniques and security measures to protect airplanes and airports from criminals and terrorists to ensure traveling safety, is strongly required for aviation industry. It also concerns all illegal activities related to air transportation as well as the high-risk environment of this sector (Ghobrial & Irvin, 2004).

In particular, the devastating events of September 11, 2001, showed how vulnerable the aviation industry was to terrorists. The tragedy of this event has heightened people's awareness for the need to consider security risk in the course of analyzing the overall system. Many governmental and commercial organizations in different countries are now taking steps to explicitly model each other's security measures.

Before September 11, because both government and commercial airlines had been unsuccessful in taking sufficient security measures, terrorists were able to identify the vulnerabilities in the aviation systems easily and develop new strategies for attacking a country through aviation, which had a greater impact than any other methods that they had used (Einav, 2003). In fact, before 9/11 Al-Qaeda had attacked American interests several times in different countries. In 1993, they attacked to the World Trade Center using a truck bomb, but its consequences were not as significant as those on September 11. Although the aim was the same, changing the means and attacking via aviation caused more damage and drew more media attention. Just this example can explain how dangerous the attacks by means of aviation can be (Stamper, 2002). Interestingly, the event of 9/11 destroyed people's confidence in the United States, which had been perceived as one of the most secure places against terrorism in the world.

September 11 was the turning point in terms of aviation security because it showed people all over the world what terrorists were capable of doing and how the security system in the aviation sector had many deficiencies and loopholes. After this event, every policy was reformed and changed radically. For these reasons, to learn the components of successful aviation security, one must consider and evaluate carefully pre and post September 11 policies and their implications.

The Transportation Security Agency (TSA), established after September 11 to coordinate all security issues in aviation, is trying to develop strategies to raise the security bar. It recognizes the need to improve its ability to create scenarios that terrorist organizations may use in attacks. TSA`s Office of Threat Assessment and Risk Management is working with economists to analyze the costs vs. benefits of the precautionary measures. Moreover, it is currently developing a project called the TSA Vulnerability Assessment Management System (TVAMS) to collect critical threat and vulnerability assessment data as a response to problems in aviation security in the United States (Berrick, 2003).

Although many precautions have been taken, there are still many defects in the aviation security systems and its related legislation (Bailey, 2002). According to their regular risk assessment measures and tests, the General Accountability Office (GAO) found that aviation industries and governments are still not prepared enough to deal with the growing terrorist threats in the world (Berrick, 2003).

The prevalence of terrorist activities around the world indicates that there is an urgent need for a stronger risk management system that can better evaluate the vulnerabilities of aviation security systems, identify possible threats, and reduce the impact of terrorist and criminal attacks.

Research Purpose

Generally, most organizations design their security programs in accordance with a rigid and rule-based approach. After an incident that penetrates the security system takes place, new rules are developed and implemented to prevent a repetition. However, as we have recently observed on September 11, the effects of a breach of security can be tragic. Therefore, governments and agencies should not wait for new types of incidents to occur and then improve their security systems. They must be more proactive in trying to predict the numerous types of security threats and take necessary steps to prevent these attacks from happening in the first place, which means that they need to consider the risks when they make decisions about security management. In order to highlight these issues, this study addresses possible threats from terrorists and criminals against the aviation industry. The risks of such threats are assessed to determine if existing security measures and safeguards are adequate or need improvement.

Transportation via aviation has inherent risks and is vulnerable to all threats due to its own structure. Planes transport not only people but also cargo, both of which are important to countries and individuals. In addition, because of improving technology, terrorists and criminals have gained many opportunities to attack the aviation industry in a great number of innovative ways. To eliminate this problem, aviation security should be checked and undergo risk assessments regularly to prevent any future possible attacks. The purpose of this thesis is to address these problems and offer possible solutions to deal with terrorist and criminal attacks. This thesis is an attempt to identify solutions to the problems that pose a significant danger for human beings and economic structures in the future.

Research Questions

Considering this background, my research questions are:

1. What are the current risks and threats to the aviation industry?
2. What is the impact of attacks against the aviation industry?
3. What are the aviation security policies in the United States pre and post September 11?

4. What are the implications of post September 11-aviation policies that have been implemented in the United States?
5. What are the strengths and weaknesses of pre and post September 11 aviation security policies?

Overview of the Following Chapters

This study contains five chapters. Chapter 1 involves the introduction, the research purpose, and research questions. Chapter 2 discusses the methodology and limitations of the study. In the methodology section, the design and procedure of this study are explained. In the second section, inevitable limitations are mentioned.

Chapter 3 comprises two sections that examine risk assessment factors in order to explain and answer the first two research questions. Vulnerabilities of aviation security are explained to show what areas of the aviation industry has risks from criminal and terrorist threats. In addition to drawing a general picture, the following factors are described in detail: target options in terms of numbers in the aviation industry, lack of international security standards in providing aviation security all over the world, insufficient security systems in general in the aviation industry, vulnerabilities of computer systems in aviation, and unintended consequences of measures that were taken after attack against the aviation industry, and types of criminal and terrorist threats. In addition, the impacts of attacks against aviation are explained.

Chapter 4 describes the pre and post September 11 security policies to answer the third and fourth research questions, and evaluates these policies to answer fifth research question. First, pre-September 11 aviation policy implementations and legislative regulations are presented by examining their historical backgrounds and different perspectives in addition to describing terrorist attacks to the aviation sector in a chronological order. Second, post September 11 policies are described to indicate what measures were taken and what policies were implemented and to understand the dimensions of risks in the aviation sector and what the policy makers did to the manage risk to aviation security. Third, both pre and post September 11 policies and implementation are evaluated in terms of their effectiveness and consequences.

Chapter 5 consists of the recommendation and conclusion sections. This chapter indicates components of successful aviation security policies by discussing several recommendations corresponding to risk assessment of aviation security. It points out the solutions, which might be appropriate for aviation security to manage these risks in aviation sector. Finally, the conclusion section wraps up this study.

CHAPTER 2

METHODOLOGY

Methodology

The method used in this study is a comprehensive literature review. In this study, much of the research is library-based. All of the information presented in this study was derived from available sources, such as University of North Texas (UNT) library card catalog and electronic research database. While investigating this subject, keywords related to this study were used to search in various electronic databases, including EBSCO Host®[1], ProQuest®[2], FirstSearch®[3], Lexis Nexis®[4], Sagepub®[5], Jstore®[6], and NetLibrary®[7]. Found articles were screened to determine their relevance to this study.

In addition, related books, journal articles, administrative and legal documents, some dependable resources from the Internet, and government websites were examined. After obtaining necessary information and exploring the relevant historical, legal and structural data, the data were categorized into a corresponding research question.

This study is designed in accordance with qualitative risk assessment methods. The purpose of risk assessment is to define and control any risks that may affect an organization (Conrow, 2003). Risk assessment is a systematic process for describing the

[1] EBSCO Industries, Inc., http://ejournals.ebsco.com/Login.asp
[2] ProQuest Information and Learning Company, www.proquest.com
[3] OCLC Online Computer Library Center, Inc. www.oclc.org
[4] Reed Elsevier, Inc., www.lexisnexis.com
[5] Sage Publications, Inc., www.sagepub.com
[6] JStore, www.jstore.org
[7] OCLC Online Computer Center, Inc. www.netlibrary.com

risks related to threats and dangers (Koller, 1999). Generally, risk is a measure of the potential for loss in terms of both the probability of the occurrence of that loss and the consequences of its happening (Conrow, 2003).

In terms of aviation security, it provides a systematic approach for evaluating risks and making decisions associated with aviation security measures. It involves the current review of technical design and/or policy decisions, and the identification of potential areas of risk. It may also help allocate funds more appropriately.

In terms of the qualitative risk assessment process on which my study is based, there are three factors that determine the concept and implementation of risk assessment: risk identification, risk measurement, and risk management (Cucchisi, 2004). In this study, while these processes are explained respectively, evaluation of pre and post September 11, 2001, aviation security policies are evaluated after the risk measurement phase to illustrate risks and impact on the security organizations more clearly.

Risk Identification/Analysis

Risk identification is determining what is at risk and its vulnerabilities and sources of threats. In this study, this process is explained by identifying the most probable threats and analyzing the vulnerabilities of the aviation industry to these threats. Basically, this process determines where vulnerabilities may be greatest and where security attention should be focused initially. The threats in the aviation industry relating to any terrorist or criminal’s attack, which could be reasonably expected to result in serious harm to at least several people, are examined respectively in this study. It also involves evaluating existing inherent risks and whether security measures can adequately oppose the potential threats to the organization.

Risk Measurement

Determining the consequences and impact of the risk constitutes the risk management phase. In this study, the impact of attacks are explained in four basic and important areas, the effects of the media, the psychological impact on victims, the economic impact on both governments and private companies, and the political impact after these attacks.

The September 11 terrorist attack is discussed between the risk measurement and risk management phases to illustrate the dimensions of possible risks to the aviation sector. September 11, which was the turning point of security risk assessment applications, is examined in two steps; previous security policies and post precautionary policies.

Risk Management

Risk management is determining the appropriate solutions to manage the risk. Basically, this process involves four alternatives to reduce risk in that organization. The first is avoidance or discontinuing the practice that creates the risk. The second is mitigation or performing some strategies to reduce the impact. The third is transfer or spreading the risk by having private insurance help pay for the cost of damages. The fourth is acceptance or learning to live with the risk. This study addresses these four-risk management phases accordingly. After evaluating pre and post September 11 aviation security policies, recommendations that propose mitigation, transfer, and acceptance of risks as part of risk management are explained.

Limitations

Due to the complexities of the issues related to the subject, some unavoidable limitations come into play while drawing a framework for aviation security. First, it is difficult to use the words “successful aviation security” because measuring the success is difficult to undertake. There is no way to know how many incidents and how many accidents can be prevented by implementing these policies, precautions and efforts. For aviation security, the successes are generally unseen, yet failures are always noticed by people because the results are so tragic.

Second, another limitation of this study is confidentiality because the concept of security issues, especially after September 11, is highly restricted in the United States due to national security concerns. Agencies do not explain every detail of policies for fear that terrorists may obtain them. Some policy implementations may not be available to the public. Therefore, the validity and reliability of the sources from which information is gathered can be questioned.

Third, the concept of aviation security is very large and broad, so there may be some deficiencies while determining its size and narrowing the scope of the subject. In addition, there are limited empirical studies on this comprehensive subject.

Fourth, the recommendations discussed in this study may not be a remedy for all countries due to fact that their structures of aviation security systems are different.

Fifth, the recommendations mentioned in this study may not be the “silver bullet” for aviation security. Some problems may be observed while implementing those issues. Nevertheless, these appear to be logical conclusions after causal analysis of the aviation security system in the United States.

Sixth, risk assessment is based on all possible scenarios or mirror imaging, so it is possible that it may exaggerate the situation by considering every detail of vulnerability. Some of the evaluations may not be practical in a real environment.

CHAPTER 3

RISK IDENTIFICATION/ANALYSIS OF AVIATION SECURITY AND RISK MEASUREMENT

"Know the enemy, and know yourself, and in hundreds of battles you will never be in peril." The Chinese general Sun Tzu made this statement over 2,500 years ago. In order to set up different levels of protection in the aviation industry, those responsible for that security must assess and understand the threats facing the aviation industry. Then they must examine the inherent vulnerabilities of the systems that were designed to protect the people who may be subjected to those threats (Whitman, 2003). In terms of security, every part of the aviation industry has its own risk tolerance and management styles.

Vulnerabilities of Aviation Security Systems

Vulnerability is a measure of the likelihood that precautions against various problems or damages will fail (Conrow, 2003). Aviation security also has numerous vulnerabilities including inherent risks of aviation. This section addresses the first research question: what are the current risks and threats to the aviation industry. The vulnerabilities of aviation security are:

Target Options in Terms of Numbers

Typically, one major factor that increases the risk is the number of targets. The more vulnerable targets you have the more risks there are. Conversely, it is easy to manage the risk effectively for a small number of vulnerable targets.

Today, 2 million passengers travel by airplanes everyday using both domestic and international airways and 450,000 millions of tons of cargo are carried by aviation companies in the world annually. There are 25,000 commercial airlines and 1,500 commercial airports around the world (Thomas, 2003). These numbers reveal the fact that protection of aviation facilities is inherently very difficult and complex; on the other hand, attacking these targets is a relatively uncomplicated task facing terrorists and criminals. Terrorists and criminals, generally, perceive aviation facilities as areas where they can find large numbers of people and insufficient security (Wilkinson & Jenkins, 1998).

An air traffic network plays a significant role for many people including businessmen and tourists around the world. It delivers critical service for people and companies in addition to saving them time. Airports providing air traffic networks are also crucial and relatively small places where a large number of people have to come together while pursuing their work and leisure. This scheduled air travel has economic, political, and social meaning for not only governments but also commercial interests (Bailey, 2002).

Therefore, when terrorists and criminals make rational cost-benefit analysis, they do not hesitate to choose these places because they can kill the maximum number people and damage a large amount of infrastructure by using a small number of explosives with relatively little effort (Thomas, 2003). On September 11, 2001, more than 3,000 people were killed; similarly, 1,732 people were killed in 70 bomb attacks by means of aviation from 1969 to 1989. The potential for huge casualties in any attack to the aviation industry causes this industry to be a preferred target for terrorists and criminals.

Thus, it is undeniable that there are high-potential risks in the aviation sector due to the fact that there are many options and ways to attack them because of the huge numbers of airplanes, airports, and aviation facilities (Einav, 2003).

Lack of International Security Standards

A lack of standardization in terms of responding to and suppressing the risks also cause the level of the risk to increase. Notably, with respect to managing the risk for aviation security, it is crucial not to leave any gaps within the system while securing the airports and airplanes.

Aviation security should be handled cooperatively by every country, not just an individual country. Growing globalization and increasing competition for tourism among countries have improved and increased international flights (Coshall, 2003). The volume of import and export among countries via aviation cargo systems has become a crucial part of the global economy. Although many international conventions dealing with aviation security have been organized and many regulations have been made, there is no comprehensive and sufficient international aviation security system in the world today. Moreover, the "it can not happen to me" syndrome is prevalent all over the globe. These situations and lack of prosecution standards among countries allow criminals and terrorists to attack by crossing international borders and choosing the aviation industry as a target. In addition, in today's global society, they can easily change their locations from one country to another because of this deficiency in security on the international level (Einav, 2003).

A terrorist may mislead the security guards and penetrate an airport in a country that lacks security. An armed terrorist may get into an airplane that is going to another country with a secured airport. After that specific airplane's pilots talk to the air traffic controller, the terrorist may hijack the airplane with his weapon, or after seizing control of the cockpit, he may change the direction of the airplane as it is being landed. This hypothetical scenario indicates that even if a country takes all precautions in their airports and airplanes, such as hiring air marshals or installing the latest technological equipments and screening devices in the airports, the security flaws in the systems in other countries may result in tragedies. In response, the U.S. has developed the CAPPS II program to collect information on passengers on airplanes from foreign countries. However, it is not feasible for such a program to solve the problem completely because there is no organization in the world that knows all the names and features of all the terrorists (Thomas, 2003). This case shows how at risk the aviation sector is without international standards.

Except for some countries that have made agreements to cooperate, most of the countries in the world have their own rules and security procedures. In addition, international terrorist organizations and organized crime groups have established networks around the globe, and today's communication systems allow them to quickly communicate and develop new strategies and actions in response to changing situations (Pillar, 2001).

In addition, a standard and universal law enforcement system around the globe has not been established up to now. Although the International Civil Aviation Association (ICAO) attempted to resolve the conflicts between countries over the problem of jurisdiction and to settle upon a system internationally, there are not any binding and effective regulations in the world as yet. As a result, without standardized regulations around the globe, law enforcement loses its deterrent effect on criminals (Dempsey, 2003a).

Insufficient Security Systems in the Aviation

Insufficient security systems in the aviation industry and the sensitivity of aircrafts to attacks are the other important factors that make aviation a good target. According to Wilkinson and Jenkins (1998), terrorists have been successful 85% of the time when they tried to hijack an airplane in the last decades. Similarly, according to the statistics, terrorists have achieved their goals 76% of the time when they attack airplanes and airports.

On September 11, the 19 hijackers' success rate for defeating the system was 100%, which indicated that they had analyzed and learned the vulnerabilities in the security systems in four airports. Between October 2001 and February 2002, there were 35 airport terminal violations involving illegal entrance into the secure area of an airport (Dempsey, 2003a).

After the September 11 attack, it became clear that hijackers could learn the defects in the aviation security systems from publicly available materials. Generally, by learning the weaknesses of any system of a target country, terrorists can develop strategies and methods for defeating them. Particularly, the question of why Al-Qaeda chose the aviation industry as a means of attacking to the United States in spite of the fact that they had not ever used the method before should be reevaluated (The 9/11 Commission, 2004).

Moreover, security measures are not limited only to the inside of the airports and airplanes. The perimeter security systems, hangars, office buildings, gas stations near airports, and accessibility of the airports may also increase the risk of the aviation industry. For instance, Dempsey (2003a) stated that the Department of Transportation (DOT) Inspector General found that illegal access to secured areas of the airports happened 68% of the time in 1998-99, and 30% of the time in 1999-2000 in the United States.

It is also claimed that since September 11, the U.S. government has spent a large amount of money on internal security, screening machinery, and x-ray devices but has overestimated the effectiveness of the perimeter security system. If the perimeters of unsecured airports were defeated, terrorists would have a considerable opportunity to attack airports by various means. Even damaging the lighting system adjacent to a runway may result in a disaster for airplanes (Sweet, 2002).

In terms of the accessibility of an airport, Dempsey stated that unlike many airports in European countries, the connectivity of United States' airports' to the inner-cities are not sufficient enough although there is an overwhelming number of airports in the United States. This access problem stemmed from either insufficient rail system or lack of other means of transportation (2003a).

Vulnerabilities in Cargo

The aviation industry carries billions of tons of cargo each year by means of passenger and cargo airplanes (Ghobrial & Irvin 2004). Moreover, it is estimated that air cargo shipment will continue to grow substantially within the next ten years. For instance, in the United States, it is expected that air cargo shipments will increase by 49% domestically and by 86 % internationally. Air cargo constitutes 29.7 % of the value of international trade. These large volumes of cargo bring their own vulnerabilities at the time of transportation. TSA assesses that the likelihood of possible bombing attack against a passenger or cargo aircraft is around 35%-65% and thinks that cargo is one of the main targets for terrorists according to the intelligence it has obtained (Elias, 2003).

The likelihood that a cargo may be tampered with while it is being transferred from its original truck, held for screening in the airport sorting centers, loaded onto an airplane, or unloaded from an airplane is very high. Passenger airplanes, in general, have been the main concern for air cargo security during the reorganization process after the September 11. However, there is also potential risk for all-cargo operators' aircrafts, such as UPS™[8], DHL™[9], and FedEx®[10] Airways (Elias, 2003).

[8] United Parcel Service of America, Inc., www.ups.com
[9] DHL International GmbH., www.dhl.com
[10] FedEx Cooperation, www.fedex.com

The types of risks for air cargo security vary. Placement of explosives aboard the airplane, unlawful shipments of dangerous materials, criminal activities which appear in the form of smuggling or theft, hijacking and sabotage by terrorists are just some examples of risks in air cargo security. In terms of placement of explosive onto an aircraft, some special explosives and incendiary devices which are undetected and placed among shipped materials are the main potential threats to aircrafts. Hazardous materials are typically not permitted aboard a passenger aircraft. However, some of them can be shipped by air if they are packed properly and they do not exceed a specified amount or number. The risk arises when the personnel handling the cargo are not truthfully informed of the nature of the cargo. Criminal activities which happen in the air cargo section appear in the forms of theft of merchandise, transportation and smuggling of contraband, forged materials, and pirated goods via cargo (Elias, 2003). In addition, personnel who deal with the cargo can also be potential risks because they may be susceptible to bribes (Thomas, 2003).

After every single terrorist attack targeting the aviation industry, authorities tend to increase the level of airport security immediately. Then when people and the media shift their focus from this subject, everything returns to its original state afterwards. The General Accounting Office or GAO (2002) stated that although aviation security systems have received great investigations and reconsiderations, vulnerabilities still exist in the security procedures for the cargo section in this industry. For instance, in terms of security measures in air cargo and freight carriers, background investigations of most employees who handle the cargo are still not complete. By the same token, the TSA found many security violations in their regular inspection tests in aviation facilities (GAO, 2002).

Moreover, today's economic conditions require fast shipping for most products because of the economic treaty between companies, deterioration of things, and the increase in production and consumption. However, especially after September 11, the screening process has increased the waiting time at the airports. Therefore, some big companies may put pressure on the government to ignore some of their products in the screening process. This condition also contributes to the vulnerabilities of the aviation sector.

Transportation of mail via air is another potential risk for air cargo security. Most unlawful materials, such as explosives, hazardous materials, and materials which are subject to prosecution, may be sent by airmail. After September 11, materials consisting of poison were sent by mail arbitrarily in the United States. Another challenge in this area is people's rights to privacy as guaranteed under the Constitution. If mail is sent by express mail, priority mail, or first class mail, they are considered as private materials which makes it difficult for agents to inspect them (Elias, 2003).

Vulnerabilities in Airplanes

Commercial airplanes are designed for peaceful conditions. Instead of security concerns, the comfort of the passengers, effective fuel consumption, and ergonomic design are given consideration in its manufacture. This creates more risky conditions for airplanes in civil aviation.

Despite the fact that many precautions have been taken by the TSA, for instance, cockpit doors have been strengthened in many airplanes since September 11, there are still a lot of vulnerabilities in the planes. Before September 11 by simply using a small box cutter or a knife, terrorists were able to hijack an airplane. Airline companies had advised the pilots not to struggle with the hijacker, but rather to summit to their demands to protect both the plane and passengers. Therefore, entering the cockpits had never been an issue for the hijackers.

As an implementation of TSA after September 11, hiring air marshals seems to be a solution to this problem; however, considering the number of flights, completely removing the vulnerability of planes is still impossible (Thomas, 2003). One must consider that the few security measures in place for an incident that appears while the planes are in flight leave the planes quite vulnerable.

Vulnerabilities in General Aviation

Many people around the world including the U.S.A. have their own private airplanes some of which are designed and manufactured by their owners. Crop dusters, along with private airplanes, number 200,000 in the United States, and they are another strong vulnerability for the aviation industry. Although the airplanes in general aviation are relatively small compared to commercial aircrafts, they may also cause substantial damage if they are misused by criminals or terrorists (Szyliowicz, 2004).

Typically, most of the planes in general aviation are stored in hangars near the airports, but some of them may be located on private land and fields. Wherever they are located, there is a high potential for theft of these airplanes. It is so open to the threats that even a teenage flight student can steal a single engine airplane as seen in Tampa, Florida in 2002. Moreover, these kinds of airplanes are also hardly recognizable by radar due to their ability to fly at low altitude. Due to a lack of sufficient security systems, these airplanes create vulnerability in the aviation sector (GAO, 2004).

If they are rented by a terrorist or criminal who is intent on attacking some important target, then nothing can be done to stop him. Background checks are not part of the requirements made on people who want to rent them (Szyliowicz, 2004). Interestingly, the September 11 terrorist, Atta, was interested in crop dusters and tried to learn how to use them before the attack. His motivation for studying crop dusters was to learn the vulnerabilities in general aviation. Some experts claim that his plan was to use a crop duster to carry gasoline, which releases 15 times more energy when mixed with air than TNT, and attack the same targets in the United States (Thomas, 2003).

Lack of Intelligence Sharing and Cooperation

Intelligence has always been an important and enduring part of governments. Operationally, it has two important roles. One is gathering information and then converting it into meaningful and useful data, and the other is implementation of this data where national security is concern. However, it is also related to international security when governments combat terrorists or organized crime groups that have connections among different countries.

A lack of sufficient intelligence, not sharing existing intelligence among agencies and a lack of cooperation among agencies which handle aviation security are the other factors that increase the vulnerability of the aviation sector. In order to identify the potential threats, protect aviation facilities from terrorists and criminals, and respond to emergencies in a timely manner, the need for intelligence is vital for any country in the world. In terms of intelligence, one of the weakest security factors on September 11 was a lack of a system that allowed the FBI and other agencies to share their collective knowledge (The 9/11 Commission, 2004).

Thus, due to the effects of globalization, many mutual or multilateral intelligence-sharing agreements have been made, both formally and informally. For these reasons, the U.S. government has made an agreement to cooperate with 400 different foreign intelligence services and security and law enforcement agencies. While the government has increased its cooperation with other countries, it has neglected to create a intelligence sharing system at home. For instance, the care of September 11 is commonly exemplified as a failure of the U.S. intelligence community to share its data (Herman, 2002).

Therefore, the intelligence community has been under observation in the United States since September 11. By and large, the criticisms were related to not collecting enough information before that tragic event. However, some people stress that even if the necessary intelligence had been collected, this event would have happened any way due to the fact that the agencies were not sharing information among themselves. For instance, although two of the terrorists in the 9/11 attacks were on the Central Intelligence Agency's (CIA) watch list, they were allowed to board the airplane because the Federal Aviation Administration (FAA) could not access the CIA's watch list. Before September 11, there was no sharing of intelligence among the airport and airline security officials and the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), FAA, and Immigration and Naturalization Service (INS). To rectify this problem, the Office of Homeland Security has been established in the United States in 2002, but this highly authoritative department needs time to work effectively to organize all these intelligence departments in the U.S.

Generally, the response to threats to the aviation industry has been reactive and defensive in nature due to there not being a having common security strategy and cooperation among agencies. As an example of lack of cooperation between agencies, The Federal Aviation Administration (FAA) and North American Aerospace Defense Command could not develop a preventive strategy on 9/11 because their individuals protocols did not cover this kind of attack (The 9/11 Commission, 2004).

Forgery and Deception

Forgery and deception are common risks for most security organizations. There are many different ways to use forgery and deception to penetrate the security of a particular organization. Criminals can forge formal documents, such as passports, birth certificates, and security passes. In terms of aviation security, forgery of passports, identity theft, stealing aviation personnel's uniforms, and providing wrong address are some of methods of deception that the criminals and terrorists may use. All these deceptive actions increase the vulnerability of aviation security (Thomas, 2003).

The forgery of passports, one of the most common acts preferred by criminals and terrorist, is a problem that threatens the security of airports substantially. By misusing an official travel document or passports, terrorists and criminals can travel from one country to another without being recognized and captured. Criminals and terrorists on watch lists are followed from the time they purchase tickets to prevent their possible illegal actions. In the United States, the FAA has prepared a watch list since 1990, and under CAPPS II program, TSA checks every name on the passenger list regularly with its computers which has links to law enforcement databases (Ravid, 2004). However, in the situation of forgery of passport, all these efforts may not work due to misleading the officers by a fake identity.

Basically, a passport permits its user to travel to other countries or come back to their own country. It may also be used as an identity card in the foreign country. In terms of aviation security, a fake passport may cause unpreventable damages in this era of terrorism. If a passport is designed professionally, it makes it difficult for a terrorist to be recognized at the immigration gates, whose personnel have to deal with an overwhelming number of passports on a regular basis. Most countries in the world have developed passports that are difficult to forge. However, there are also some countries whose passports are fairly weak in terms of security and can easily be forged.

It is certain that some terrorists or criminals may benefit from this condition and attempt to travel to those other countries.

Thefts of flight crew uniforms and credentials are the other vulnerabilities of aviation security in terms of forgery and deception. The Airline Pilots Association has warned the pilots and security guards that terrorists may emerge with pilots' uniforms that may have been stolen or may have been manufactured based on original ones. Moreover, the name of the pilot, which is presented on the uniform, may also be obtained from the list on the Internet because the FAA put all the names of pilots into the website (Thomas, 2003).

Easy Target for MANPADS

Shoulder-launched surface-to-air missiles, the Man-Portable Anti-aircraft Defense Systems (MANPADS), are recognized as a serious threat to aviation security systems. Predictably, there are 500,000 MANPADS in the world today, many thousands of which are thought to be on the black market and therefore accessible to terrorists and criminals. Their portability and concealable features make MANPADS dangerous and hard to detect. These weapons have a four- mile range and 15,000 feet capacity, so they may be used to attack airplanes easily.

Typically, they are fairly inexpensive, but extremely lethal. In addition, if trained properly, a user can use it well. Because their features enable them to be launched far from airplanes, they may be used to attack airplanes without any warning. Since 1970, 42 aircrafts have been attacked and 29 aircrafts have been damaged by this weapon.

Furthermore, terrorists have begun to use this weapon to attack commercial airplanes in non-combat zones around the world. For instance, in 2002, terrorists attacked a commercial airplane in Kenya by using this weapon (GAO, 2004).

If trained terrorists use this weapon against unprotected airplanes, the result of this kind of attack, without doubt, is tragedy. Moreover, this weapon's countermeasures which can be installed on airplanes are very expensive and time consuming. Thus, MANPADS form a considerable risk to civil aviation (Szyliowicz, 2004).

In terms of access assessment, when compared to other highly visible targets such as nuclear plants and high profile government installations, airports are public spaces and easily accessible to everyone. Terrorists can even attack the airports from nearby highways, which also increase the vulnerabilities of airports. History is fraught with examples about people who entered the airports from its weak perimeters and later fled to another country (Bailey, 2002).

Moreover, terrorists can gain a large amount of information, including maps and scaled drawings of airports, newly regulated aviation security systems, and the features of avionics and computer systems in the airplanes from the media and the Internet (Greenberg, 2003). Besides their current political agenda, terrorists can also use the Internet to post information on how to make bombs, biological, chemical, or other unconventional agents. Moreover, some documents that show the vulnerabilities of the aviation security systems, such as GAO Reports, are open to the public. Any terrorist can learn these deficiencies in the aviation security system and can take advantage by paying close attention to publicized details (Pillar, 2001).

Vulnerabilities in Aviation Computer Systems

The vulnerabilities of computer systems in aviation are also important factors that terrorists and criminals when considering airplanes and airport facilities as targets. As stated at the International Conference on Aviation Safety and Security (1997), most computer programs and operating systems have authentication problems and can readily be misused by others (Neumann, 1997).

Aviation security highly depends on computer and infrastructure networks, such as electric power, air traffic control, and telecommunications. Computers are used to store vital information, such as watch lists, passenger information, flight information, and personnel information. Vulnerabilities of the computer stem from various factors including software problems, accidents, troubles in data processing, and deliberate attacks (Nordwall, 1997).

In the world of computer hackers, attacking computer programs is relatively cheap, not very dangerous, and easy to accomplish. Any mistakes in software programs, such as inaccurate configuration or incorrect use of a function or command, can result in security problems. If any misuse happens, many inevitable and fatal results may appear in aviation. These include loss of confidentiality, pause of air traffic control services, closing of airports, loss of airplanes, refusal to accept services, and loss of data integrity.

Typically, cyber attacks are difficult to resolve and the attackers are rarely captured. Currently, there is no firewall that can prevent the systems from all cyber attacks completely (Nordwall, 1997). Moreover, it is also hard to recognize whether problems are caused as a result of an attack or not. To determine what causes the problem, many alternatives should be checked. If a cyber attack targets aviation security, it may also be difficult to resolve because investigators have to work a lot to identify all the parts of a physical attack, such as the sabotage against Pan Am Flight 103 (Mann, 2002).

In aviation history, there have been several attempts to damage aircrafts by changing flight courses via penetrating radio frequency systems. Computer related aviation accidents, such as the downing of the two U.S. Black Hawk Helicopters by an F-15 fighter in Iraq and the crash of an American Airlines flight in Colombia, indicate that terrorists may cause lethal damages by penetrating computer systems in the aviation industry. Electromagnetic interference may also be evaluated as an alternative way to harm an aviation computer system (Neumann, 1997).

TSA, continuously, must communicate with private companies to get necessary passenger information into the CAPPS II program. This communication is kept by computer networks.   Even if the government side takes all necessary precautions against cyber attacks, private companies may not be equipped with comparable protection systems. This situation may also create vulnerability in the system.

During flight, cellular phones and any toys controlled with remote controls are prohibited because they emit low-level interference, which can cause damage to the plane's gyroscopic systems, used for monitoring the conditions of the airplane. However, the use of laptops is allowed during flight provided they are not connected to the Internet. In spite of the fact that they are checked in separately at a security checkpoint, some mechanism can be inserted into a laptop to send signals to damage an airplane's electromagnetic systems (Thomas, 2003).

The air traffic control system, including computers, communications, and radars are one of the most vulnerable targets in the aviation industry. Every flight depends on these systems and any attack against them can cause uncontrollable damage (Neumann, 1997). The General Accounting Office (GAO) (2002) stated that most aviation facilities had not prepared risk and threat assessment analysis for 5 years prior to review. With respect to software security, there are some claims that the FAA did not regularly conduct background checks for employees who repair and inspect high security computer systems. If any information leaked out from them to any terrorist hackers, the damage would be more devastating than September 11. Unfortunately, the threats still exist because of the vulnerability of these systems (Coughlin, Cohen, and Khan, 2002).

In addition, electronic and electromagnetic protection measures should also be considered in the screening areas of the airports because the detection devices for screening may be damaged or disabled remotely by terrorists. Electronic deception, which deliberately makes radiation, alteration, or reflection of electromagnetic energy to give misleading information or deny valid information, and electromagnetic interference are some techniques that terrorists and criminals use in their attacks. Therefore, electronic security is also part of the risks of aviation security (Neumann, 1997).

Unintended Consequences of Measures

Unintended consequences of these precautionary measures also have potential risks for the aviation systems. For instance, armed pilots and air marshals have been assigned to struggle with possible threats in the air. However, the human factor may produce unexpected results during or before the flight. Many scenarios or strategies can be developed by terrorists who can not bring their own guns onto the airplanes. For example, if pilots open the strengthened cockpit door during flight to use the lavatory, hijackers may take advantage of this situation. They can enter the cockpit and gain control of the airplane by locking the strengthened doors, which would prevent anyone from entering. The strengthened door then becomes the tool of the hijacker (Thomas, 2003).

In addition, even though the government and commercial airlines are taking these precautions for people’s security and safety, some people have concerns about protecting their civil rights, including the right to privacy (Haque, 2002). They claim that the new regulations limit privacy rights and decrease the government’s accountability (Ghobrial & Irvin, 2004). For instance, the policy detailing “Sensitive Security Information” (SSI) allows TSA to hold any information if revealing it would be damaging to the security of transportation. Thus, some people claim that this rule superseded the Federal Freedom of Information Act.

Similarly, some ethnic-minority groups claim that they have been exposed to intolerant and aggressive behaviors at the airports. Predictably, screening workers at the airports focus more on some ethic groups, such as people from Middle East. However, since discrimination in such cases can be evaluated as a violation of civil rights, terrorists may want to take advantage of this condition and make propaganda against that country (Cobb & Primo, 2003).

Creating "trusted passenger" programs to accelerate the screening process may be beneficial at the airports. However, trusting too much in a known shipper program, which gives some privilege to a private company making business via airplane many times, may cause unintended consequences. Terrorists may want to penetrate the system via these companies (Campbell, 2002).

New Forms of Crimes

Another vulnerability of the aviation industry is the derivation of new forms of crime, such as bio-terrorism, which first appeared immediately after September 11 in the United States Postal Service (Miller & Heldring, 2004). Millions of people have to pass through airports and fly airplanes. For this reason, international airports especially are seen as a perfect target by terrorists who want to harm many people.

In today's world where suicide bombers have been seen in many corners of the world, it should be taken into account that biological and chemical agents could also be used to bring down an airplane during flight (Thomas, 2003).

Distribution of infectious diseases is one of the possible actions of terrorists, who can easily do it in these crowded areas. If a terrorist carrying a disease enters a country by passing through its airports, he may threaten millions of lives. This disease can be distributed all over the world in a few days (Thomas, 2003).

Many experts agree that a terrorist who brings in chemicals or is a carrier of a deadly virus and bacterium can be a lethal weapon. For instance, there are 123 chemical plants in the United States. If any assault was committed against these places, each of the chemical plants could expose over 1 million people to toxic gases. After September 11, America became really worried about an anthrax attack from Al-Qaeda.

Currently, 600 tons of nuclear material, most of which belonged to the former Soviet Union, remains unsecured in the world. If terrorists obtained some of these nuclear materials, the result would be catastrophic. In addition, a vast majority of the developed countries have nuclear plants and many other countries in the world seek to establish nuclear energy plants in their countries. However, some of the countries' intent is to produce nuclear weapons despite some agreements after the Cold War. These plants may cause a risk for aviation security if they are targeted for attacks by airplanes used as missiles (Miller & Heldring, 2004).

Threat Assessment of Aviation Security

Threat is a measure of the likelihood that a specific type of attack will be carried out against a specific target. Threat analysis is used to identify the sources and types of threats (Conrow, 2003). Identifying the possible threats helps executives to manage the risks. This section responds to the first research question regarding the threats of aviation security. In aviation, two groups have constituted the common threats against aviation since its inception: terrorists and criminals.

Terrorists

Typically, terrorists constitute a bigger threat to aviation security. They are more diverse, more organized, more willing to take risk, and more professional than criminals. Moreover, terrorism has become huge economic sector that has its own political and ideological objectives. Terrorists have supporters, charities, banks, specific incomes, and financial networks. They have the ability to perform sophisticated and complex operations that may affect different countries significantly (Skinner, 2004).

The vulnerability of the aviation industry always compels many terrorist groups to use it as a tool in their propaganda. Terrorists often try to obtain maximum psycho-political influence all over the world, and attacking airports and airplanes usually enables them to accomplish this goal.

According to Wilkinson and Jenkins, terrorists changed their tactics after Post-Cold War era (1998). They began to kill innocent people and exact maximum destruction on the country that they hated and wanted to terrorize. Moreover, terrorists also started trying to kill the maximum number of people, including themselves, since the sensational nature of such killing causes more media attention.

Terrorists' motivation and perspectives of life are also important reasons why they choose the aviation industry as targets. Generally, terrorists focus more on attacking the political, military and economic infrastructures in a country. The motives of these attacks may be punitive, symbolic, religious, idealistic, ethnic, political, social or economic. From such varying motivations, we can see that terrorists and criminals will perform virtually any attack on people (Butler, 2002). These attacks usually results in large civilian casualties, long-lasting economic damage, and sometimes electoral changes; for instance, Spain experienced such a devastating train attack which more than 182 people were killed and 900 wounded. This attack affected the result of its presidential election in 2004 and cause to change the politicians who supported the war in Iraq (Skinner, 2004).

The other motivation is obtaining enough money from their supporters and countries sympathetic to their causes so that they can manage their long term goals, such as going to aviation schools and gaining information about airports and its systems (Wilkinson & Jenkins, 1998). From the terrorist's point of view, by attacking highly valued and hard targets, such as the Pentagon and World Trade Center, they believe that they can gain a significant victory against a country that they perceive as an enemy. Another indirect result of such an attack is causing people in that country to lose faith in their government's ability to protect them. In such a case, terrorists would accomplish their goal of revenge against that government because fear among people and political pressure to that particular government would increase (Butler, 2002).

In addition, some terrorist organizations and criminals may want to provide clues to the media and law enforcement agencies so that they can be recognized after an attack and their message can be broadcast clearly. In doing so, they can promote their strength and demonstrate how much further they are willing to go (Coates, 2002). By the same token, most terrorist attacks contain implied messages for a target country. In the case of September 11, it was very meaningful that they attacked highly symbolic places for economic and military targets. If the fourth plane had not crashed in Pennsylvania, the target would have been the White House, which would have sent a clear political warning (Stamper, 2002).

The Department of Homeland Security (DHS) indicated that terrorists are still seeking ways to attack the United States via aviation, such as attacking chemical plants, petroleum, and petrochemical facilities, transportation systems and facilities, and electric power grids. According to intelligence sources, their aim is using commercial airplanes to perform these attacks (DHS Raises concern, 2003).

To illustrate, on September 11, one of the hijacked airplanes turned south near Albany, followed the Hudson River down to New York City and reached its target, the north tower of the World Trade Center. On its route, it passed directly over the Indian Point Nuclear Power Plant, which is located 30 miles north of Manhattan. It is not difficult to imagine that had terrorists chosen this nuclear plant instead of the World Trade Center, the effects of this attack would have been more devastating and disturbing on that day.

Criminals

The Federal Aviation Administration's Office of Civil Aviation Security's publication, Criminal Acts against Civil Aviation, indicates that in 2003, 138 aviation security incidents happened around the world, including airport attacks (32), bombings (3), shooting at aircraft (9), hijacking (57), commandeers (13), and attacks against general aviation (9).

Criminals also pose a significant threat to aviation security. According to the International Civil Aviation Organization (ICAO)' publication, Annex 17, criminal activities against civil aviation have been seen in these forms: attacking airports, commandeering of civil aviation aircraft, bombings, attempted bombings, shootings on civil aviation aircraft, shootings at in-flight aircraft, off-airport facility attacks, incidents involving general aviation, hijackings, and unlawful interference of civil aviation aircraft.

Particularly, organized crime groups, whose numbers have been increasing for the last two decades, constitute a potential threat to aviation security because they often try to smuggle guns or drugs via aviation. Airport assault, murder, and airport sabotage have also been committed by criminals. Cargo theft, armed robbery at the airport, and larceny either at the airports or on the airplane are other common criminal activities and threats to security (Sweet, 2002). Cargo theft appears in different forms, including baggage handlers stealing from passengers' luggage and armed assaults against an aircraft targeting specific cargo, such as money.

In addition, some passengers not showing normal behaviors by harassing and abusing other passengers during flight are other problems for security. Sometimes they may be under the influence of alcohol. For instance, in 2002, an airplane belonging to Air France had to make an emergency landing because of a naked passenger who wanted to control the airplane in the air (Thomas, 2003).

The Impact of Terrorists' Attacks against Aviation

This section addresses the second research question, "what is the impact of attacks on the aviation industry?" by evaluating four significant areas of impact: the media, psychological, economic, and political.

Effects of the Media

Since globalization, the role of the media has been increasing rapidly. Today, the Internet allows people to access even last minute news, so people all over the world can learn of every terrorist attack against aviation targets in a very short time. Considering its sensationalistic effect on the public, terrorists are liable to choose airports and airplanes (Einav, 2003).

Typically, exposure to media coverage of any critical event, such as an airplane collision, focuses people's attention on that event and changes their attitudes, feelings and perceptions. The media becomes a kind of 'conspirator' of the terrorists. The terrorists need the media coverage; reporters and TV producers need the stories. One of the aims of terrorists is to promote fear in the public's mind and the media is the best way to accomplish this goal (Greenberg, 2003).

After September 11, the mass media constructed an environment of fear and changed the perception of terrorism in people's minds. Instead of increasing the public's awareness for the reasons of this attack, they focused on victimization caused by this kind of attack. The notion of "everybody can be a victim" was emphasized. Thus, people began to buy guns to protect themselves and avoided traveling by airplane because of fear of victimization. It was claimed that the National Rifle Association (NRA) supported this condition and promoted fear among people to build support for this philosophy. However, the aviation industry has really suffered from this environment (Altheide, 2004).

In addition, not only did the World Trade Center have tangible value for New York, but it also had symbolic meaning for most Americans. These Twin Towers, perceived as "The soul of New York", were highly promoted and mentioned in the media all over the world. In many pictures of the New York seen in the media, the World Trade Center was shown as a dominant structure. This media attention seems to have motivated the terrorists to choose this target (Greenberg, 2003).

Psychological Impact

Attacks against the aviation industry also have a psychological impact that increases its vulnerabilities. Although terrorist attacks are evaluated by the number of deaths, the psychological effect on people should also be taken into account (Butler, 2002). Einav (2003) claimed that terrorism is psychological warfare that increases people's anxiety, fear, mistrust, resentment and reactions in degrees inversely proportional to reality. Their ultimate goals are that these emotions paralyze the community in their daily routine and increase the pressure on the government to consent to the terrorists' claims.

Particularly, children are deeply affected by such incidents. For instance, a high level of distress was found in students in the United States immediately after the September 11 attack (Auger, Seymour, and Roberts, 2004). One of the most common psychological problems after terrorist attacks is posttraumatic stress disorder (PTSD), which can be defined as long-term anxiety responses to a traumatic event that damages people's normal defense mechanisms. In the case of 9/11, many people watched this tragic event on live television, and the symptoms of PTSD have been observed in many children in the United States (Auger et al., 2004). With respect to adults, Eidelson R., D'allesion, and Eidelson J. (2003) stated that in addition to PTSD, adjustment disorders, major depression, anxiety disorders, and negative feelings about work emerged in the days following the September 11 attack.

Moreover, increased tobacco and substance use, family violence, poor school performance, increased risk taking, and other behavioral problems can be observed in the people who were exposed to serious terrorist attacks (Miller & Heldring, 2004). Traumatizing and re-traumatizing effects can be seen in people who watched this incident on television again and again, listened to stories from survivors and rescue workers, or saw this tragic event first hand while it was happening (Eidelson et al., 2003).

Generally, people affected by such events have fear about their lives, their future, and wish such attacks would not happen anymore. The only thing that they want is for precautions to be taken immediately (Burskly, 2001). After the crash of American Airlines crash on November 12, just two months after September 11, people were worried that another terrorist attack would happen again. These kinds of feelings cause people to show abnormal reaction. Peace and security, the roots of a healthy community, suffer seriously as a result. People in the U.S. had not been affected substantially till the tragedy of September 11 since World War II (Carol, 2005). Interestingly, some people may desire the dark and uncertain atmosphere following events like these because they evaluate this as a marketing opportunity. In this period, these kinds of people always try to sell some devices and software to panicked people (A must-do list, 2001).

Economic Impact

The aviation industry is one of the most important industries in the world and a market whose costs are extremely high. In the United States, which provides 40% of all flights in the world, there are 5,000 airports, 55,000 pilots, 200,000 private airplanes, 475 commercial airport supervisors, and 7,000 air traffic controllers (Szyliowicz, 2004; Thomas, 2003). These numbers indicate that not only do aviation facilities have symbolic importance, but they also have huge economic significance. In the United States, the aviation industry manages 11 million jobs and constitutes 6%-7% of the nation's gross domestic product (GDP (Szyliowicz, 2004). Basically, transportation has always been an inseparable part of the U.S economy. The United States has a service economy equipped with movable brainpower to serve immediately to the business wherever it needs. Therefore, air transportation is one of the vital points of the U.S. economy. Even though flights were canceled for only three days immediately after September 11, the economy really suffered during this short period of time (Dempsey, 2003a).

The aviation industry is very sensitive to any changes in economic cycles in the business world. Along with maintaining security, trying to reduce congestion and delays in the airports and delivering items on time for customers has major financial implications and cause problems for most aviation companies (Hale, 2002). Ghobrial and Irvin (2004) claimed that the aviation industry is usually the first to suffer the bad effects of a weak economy and the last to benefit from a strong economy. In addition, the competition between airlines also reduces the benefits of a good economy. Therefore, any negative intervention in this susceptible business may cause extreme damages.

After September 11, many aviation companies had to be closed down and a lot of people became unemployed. It has been appraised that September 11 caused economic losses of more than $70 billion (Balahadia, 2003; Hale, 2002). Unsurprisingly, one of the first groups that experienced the negative impact of September 11 was the owners and residents of the Towers and the surrounding buildings (Staring, 2003). Kim & Gu (2004) stated that worldwide commercial passenger traffic decreased approximately 18% in the year following the attack. As for the United States, commercial passenger traffic fell 40% in the same year. Campbell (2002) stated that entire aviation industry in the U.S. lost $7.7 billion, even after they received $5 billion in grants. By the same token, the Gross Domestic Product (GDP) declined 0.5%in 2001. The U.S. government spent $7.2 billion to cover the damages and other related costs (Looney, 2002). Airlines were severely affected due to economic waves in business markets and were on the verge of bankruptcy because booking rates declined by 70% (Ghobrial & Irvin, 2004).

It is clear that there were both direct and indirect significance for terrorists when choosing the World Trade Center, which was the economic symbol of the United States. They showed their success at directly striking a status symbol of a superpower. Indirectly, they accomplished their goals because increasing insurance costs, high fuel prices, and the costs of security systems have pushed the aviation industry into a troubled condition. There are several factors causing loss of revenue for airline companies:

First, one of the major economic impacts of the attack of September 11 was the profound damage to the insurance market. As a result of this impact, policyholders have faced higher costs and additional fees (Rhee, 2000). Liability insurance has increased from $2 million to $150 million annually. Similarly, according to Field (2000), tax has been raised 15% in 5 years. Today, approximately one fourth of an airline ticket price is tax, and it is likely to increase in the future. As a result of the tax increases, the demand for travel by airplanes has decreased. Thus, many airline companies have economic problems due to this high capacity but low demand environment (Ghobrial & Irvin, 2004).

Second, security expenses are also a burden on the aviation industry's shoulders. So far, $1.5 billion has been spent to increase security at the airports (Coughlin et al., 2002). Airport funds, typically, come from federal government's allowance and airline charges. Post-September 11, along with the increase in security measures, the expense of airlines also rose.

Third, federal marshals, who are assigned to protect airplanes against possible threats in the air, constitute another expense for the airline companies. They are usually placed in the first class section of the airplanes, but the federal government pays only a discounted price for them. Increasing the number of air marshals in accordance with Air Transportation Safety and System Stabilization Act (ATSA) means increasing a lost source of income for aviation companies. Fourth, before September 11, businessmen could carry their sensitive cargo onto the same plane. However, post-9/11, the amount of this cargo has been limited by the FAA. This regulation reduced 50% of demand in this area, which means another loss of revenue for airline companies.

For those reasons, dismissing workers has been perceived as the only method to reduce the operating costs of airlines. Companies have lost millions of dollars due to negative perceptions stemming from fear of air travel and increased ticket taxes. Long lines and severe security measures that use up valuable time have resulted in switching preference to other transportation systems or canceling traveling plans (Ghobrial &. Irvin, 2004).

Along with the aviation industry, numerous industries, such as the hospitality industry, in the United States have been affected directly or indirectly. With falling demands in the weeks following September 11, the hospitality industry experienced its worst periods. Many luxury hotels in New York and Boston suffered because of 9/11 events and they are still struggling with economic problems (Enz & Canina, 2002).

The aviation industry was already in a difficult condition before the September 11 attack. In fact, this sector had many financial problems, so deregulation of the aviation industry had to be implemented to remedy the economic problems in the aviation industry (Ghobrial & Irvin, 2004). In addition to these circumstances, the terrorist event of 2001 exacerbated the situation (A must-do list, 2001).

In aviation industry, reducing the economic harms of terrorist and criminal attacks is really difficult and hard to accomplish. People in aviation industry should consider various factors and endeavor to obtain economic success. For instance, to regain passenger confidence after an attack is important factor that the people in aviation industry should consider. Because of the fact that fears of transportation via aviation cause significant damage economically to aviation industry, new provisions should be developed in terms of commercially. For instance, some provisions may be provided by airline companies to constitute a reasonable and fetching transportation means (Abeyratne, 2002).

Political Impact

Attacks against the aviation industry often result in a strong political reaction and force politicians to make public speeches. Therefore, any story about an attack in aviation is usually guaranteed to be placed on the front pages of most newspapers and described repetitively (Cobb & Primo, 2003). Most of the time, all messages from terrorists can reach the public via the media to affect the politicians. This condition allows them to gain a worldwide reputation (Einav, 2003). Moreover, they can also manipulate the media to further their specific interest. After carefully preparing their images and scripting their messages, they may send video or audio materials to television companies which will not hesitate to broadcast these images (Pillar, 2001). All these manipulations of terrorists and criminals may cause politic changes in a specific country, especially during election time.

Another negative political impact is that these attacks may also initiate conflict between countries in the international arena, which in turn affects the politicians' status in that country.

Generally, terrorism is supported by militarily weak countries that desire some political changes in the target country. State sponsored terrorism involving violent actions against commercial aircraft, such as the Pan Am 103 "Lockerbie" case has increased in the last two decades. Some countries that could not establish strong and straightforward political ties in the international arena choose this kind of attacks to show their political reactions to the target country (Skinner, 2004). At the individual level, the 20th century has witnessed many hijacking incidents which were performed by political refugees who were seeking secure places (Dempsey, 2003a).

In some countries, after disasters, conflicts, or catastrophic events, the elected government may fall or is changed if the numbers of deaths reach a specific number. Since the attacks via aviation may cause devastating tragedy, it may also cause a government to change.

Summary

The security chain is only as strong as its weakest links. If these weakest links, vulnerabilities, are known, the security system can be evaluated whether it is strong or not. By using risk assessment techniques, vulnerabilities are discussed systematically to show how strong the aviation security is in the first section of this chapter. Notably, in addition to its inherent risks, aviation industry has many weakest links in terms of security. Although there are many target options in terms of numbers, security systems in aviation industry is not sufficient enough to maintain secure flight. In different elements of aviation industry, such as cargo, airplanes, and general aviation, have numerous vulnerabilities. Moreover, lack of intelligence sharing and cooperation between agencies made it difficult to overcome the threats against aviation sector. Aviation security is also vulnerable against common threats, such as forgery, deception, and cyber terrorism and crime. Moreover, shoulder launched missiles pose significant threat for aviation industry. New forms of crimes, like bioterrorism and nuclear terrorism can also be committed via aviation means. Furthermore, despite all these vulnerabilities, there is no international security standard in the world.

Second section of this chapter addresses threat assessment. Threat assessment enables us to know who can be a possible threat against aviation security. Particularly, when looking at the history of aviation, it can be discovered clearly that terrorists and criminals constitute significant threat against this sector.

In the third section of this chapter, risk measurement phase is discussed. If the possible outcomes and impacts of any attack stemming from terrorist and criminal actions are known, then it can be evaluated that how big and important that attack is. Generally, in aviation sector, the possible impacts of attacks are observed in the media, economy, and political arena. These attacks have also psychological impacts over people.

CHAPTER 4

EVALUATIONS OF PRE-POST SEPTEMBER 11 AVIATION SECURITY POLICIES

This chapter addresses the third, fourth, and fifth research questions: What are the aviation security policies in the United States pre- and post-September 11?; What are the implications of post-September 11 aviation policy that have been implemented in the United States?; and What are the strengths and weaknesses of pre- and post-September 11 aviation security policies? Most experts in the world agree that September 11 was the turning point in aviation security. It was a perfect example to show what the vulnerabilities and threats to aviation security were and the cost of ignorance. The perception of risks and the importance of aviation security can be clearly understood by evaluating what had been done before September 11 and what was changed after it. In last section of this chapter, the critics of the mistakes made by the policy makers are shown to evaluate pre and post September 11 policies.

Aviation Security Policies before September 11

The Historical Development of Aviation Security Policies in the United States before September 11

The first hijacking attempt occurred in 1931 when Peruvian revolutionaries tried to hijack a Ford Tri-motor airplane, but the first successful hijacking of a commercial airplane happened in 1948, which resulted in the crash of an aircraft in the ocean near Macao, China. In the United States, the first hijacking occurred in 1961 (Dempsey, 2003a). Later, 12 attempted hijacks had been committed in the United States by 1968.

Between 1968 and 1969, 40 hijack attempts occurred, many of which were related to Cuba. In response to these illegal activities, the U.S. Congress ruled that this kind of aviation related crimes were federal crimes and must be adjudicated in federal courts (Russell & Preston, 2004).

In 1970, Palestinian guerillas hijacked three flights by utilizing an inexperienced employee and a lack of technological support at the airport gates. However, the terrorist group, which hijacked a TWA jet in 1976 and intended to arrive at Chicago, had to use simulated weapons because of the technological improvements at the security gates and baggage screening procedures (Garvey, 2002).

As a result of these terrorist and criminal attacks, the Congress had enacted various legislative arrangements and policy makers had developed several policies in the United States before September 11. Some of these arrangements and policies that can be milestones of the aviation history are indicated below:

Civil Aeronautics Act of 1938

In terms of legislative development of aviation security in the United States, the Civil Aeronautics Act of 1938 was one the first important legislative arrangements for aviation security in the United States (Rhee, 2000). In those days, approximately, one-three of airway passengers were Americans in the world. Therefore, the government, referring to this act, established a new agency, the Civil Aeronautics Board to control and regulate security and safety issues in addition to commercial activities in the United States in 1939. Particularly, this agency was responsible for economic regulations of airline industry (Ravich, 2002). In fact, the duties of the Civil Aeronautics Board were to issue and manage aircraft and pilot certification and suspension, inquire aircraft accidents, regulate airline routes, airway facilities, control towers, airline tariff, and airmail rates, and implement aviation regulations regularly (Friedman, 2001).

In addition, it was also responsible for maintaining order in aviation industry by controlling market entry and anti-competitive implementations in this business. The Civil Aeronautics Board strictly observed airlines and enforced the regulations to prevent unfair competition among airlines (Ravich, 2002). This agency was closed in 1984 after the Deregulation Act had been enacted in 1978 (Friedman, 2001).

The Federal Aviation Act of 1958

Before the Federal Aviation Act of 1958, aviation safety and aviation security were assessed together and precautions were taken without distinguishing these two concepts. After many problems had been observed, this act separated security and safety issues for aviation in the United States into whether they were effective and economical. In the late 1960s and early 1970s, passenger screening was first initiated and begun to implement in the airports of the U.S. (Bailey, 2002). According to this act, the federal government was authorized to regulate civil aviation, but would be supported by states if the government requested to do so (Kelly, 2000).

The government, referring this act, established the Federal Aviation Agency (FAA). The FAA was assigned to implement security and safety policies in the United States. In addition, this Act transferred the authority of implementation of aviation regulations and accident investigation from the Civil Aeronautics Board to the FAA. Later, Federal Aviation Agency became Federal Aviation Administration under the new federal agency, the Department of Transportation (DOT) (Dempsey, 2003b). Before September 11, under the FAA, a special task force was established to respond to terrorism and criminal activities against airplanes that belong to the U.S.A. The special task force, basically, created a profile list to detect dangerous people and keep them away from airports and airplanes. In addition, the screening procedures and technology have been enhanced after each tragic attack against aviation. Nevertheless, attacks against aviation continued in spite of all these efforts by the FAA (GAO, 2004).

In 1967, due to concerns for national transportation security and safety, the Department of Transportation (DOT) was established to coordinate all the transportation policies in the United States. The DOT reorganized several existing agencies, one of which was the FAA, and gave them new responsibilities to provide security and increase effectiveness in the transportation. Moreover, the DOT had authority to oversee all security measurements in the transportation system in the U.S. (Dempsey, 2003b).

Anti-Hijacking Act of 1974 and Air Transportation Security Act of 1974

As a result of unpreventable hijacking trends in the world and in the U.S.A., Congress enacted the Anti-Hijacking Act of 1974 and the Air Transportation Security Act of 1974. The Anti-Hijacking Act prohibited the carrying of weapons onto a commercial airplane. Basically, this act was established to provide the requirements of Hague

Convention which regulated the extradition or punishment of hijackers in international arena. This act included punishment of people who hijack an airplane inside and outside of the United States. A hijacker could be prosecuted anywhere in the world within the U.S. jurisdiction (Dempsey, 2003a). According to this act, if a hijacker kills a passenger while hijacking the airplane, he gets 20 years imprisonment or death penalty. This act also allowed government to cancel all flights with the particular country that supported and protected the terrorists who hijacked the airplanes (Dempsey, 2003b). This act also pointed out the security problems in the U.S. airports. FAA was addressed to enhance the security to provide secure flight. FAA was ordered to check the security design and screening procedures at the airports (Dempsey, 2003a).

By the same token, the Air Transportation Security Act brought new regulations for screening procedures (Rhee, 2000). It required screening each one of the passengers who traveled within the territory of the United States. These regulations accomplished to reduce hijacking trend in the United States. For instance, in 1972, 28 U.S. airplanes were hijacked, but as a result of these legislative arrangements, only two hijacking happened between 1975 and 1986 (Dempsey, 2003a).

In addition, the Civil Aviation Security Division (CAS) was established under the Federal Aviation Administration to protect civil aviation from any terrorist and criminal attacks. This division contained two sections, one of which tried to prevent internal threats, while the other concentrated on external threats and international terrorist activities. In 1974, the Aviation Security Research and Development Division were set up. This division's aim was to use research and development programs about aviation security. This division depended on technology and contained sections that dealt with weapon detection, aircraft strengthening, human factors, and airport security technology integration (Sweet, 2002).

Aircraft Sabotage Act of 1984

In 1984, the Aircraft Sabotage Act was presented by the President Ronald Reagan and enacted by Congress to implement the rules of the Montreal Convention, which proposed regulations to terminate air sabotage. It brought many harsh sentencing against violators of aviation security rules (Rhee, 2000).

This act required to punish severely the accused people who hijack, damage, destruct, and destroy the aviation facilities including airplanes. The punishments were various from $100,000 fine to 20 years imprisonment. In addition, this act regulated the punishment process to resolve the jurisdiction and prosecution problems for crime which is committed via aviation in other countries. This act was also designed to combat international terrorism including not only individual terrorists but also some countries that support the terrorists to initiate sabotage acts against aviation facilities (Dempsey, 2003a).

International Security and Development Act of 1985 –
Foreign Airport Security Act of 1985

As for the International Security and Development Act of 1985, it gave the government $9,840,000 during 1986 to enhance security at foreign airports. Like Aircraft Sabotage Act, this statute also addressed state-supported terrorism and assigned President to establish an international cooperation to take precautions against these countries (Dempsey, 2003a). Likewise, the Foreign Airport Security Act of 1985 was an effort to solve aviation security problems for U.S. citizens who were traveling via other countries' carriers. This act also addressed the international terrorist acts which affected aviation industry economically. Moreover, in the United States, before there had been no evaluation system of other countries' aviation security whether they had significant risk to the U.S., this act created an information system to fill this gap (Manning, 1996). Government also authorized the FAA to evaluate foreign aviation systems that had flight traffic to and from the United States (Dempsey, 2003a).

After these preventive regulations, there seemed to be decrease in the number of terrorist and criminal attacks against aviation facilities in the U.S.A. until the tragedy of Lockerbie in 1988. In this event in which 259 people were killed, a terrorist put a portable radio with an explosive onto an American airplane, Pan Am Flight 103. When the plane was over Lockerbie, Scotland, it exploded and killed all the passengers and eleven people in Lockerbie (Birkland, 2004; Rhee, 2000). The method used to destroy Pan Am Flight 103 was a small amount of "semtex", a plastic explosive. It could not be adequately detected by x-ray devices because it could be formed in many different shapes, such as very thin sheets that made it difficult to detect (Schwartz & Bayer, 1992). This indicated that the FAA must continue to follow new technological developments that terrorists may invent. In 1989, according to a project conducted by the FAA, new explosive detection devices, such as the thermal neutron analysis (TNA) machine were bought by the airports served by U.S. carriers (Swartz &Bayer, 1992).

Presidential Commission on Aviation Security and Terrorism-Aviation Security Act of 1990

In 1990, the Presidential Commission on Aviation Security and Terrorism was formed by former President Bush. This commission stated that the aviation security system was flawed, so it needed to be improved (Reser, 1998). According to the Aviation Security Improvement Act of 1990, intelligence would be controlled by the Department of Transportation which would collect, manage, and refine all intelligence and information for the aviation sector and the federal security manager from this department would receive this refined intelligence at the airports and monitor the security threats (Schwartz & Bayer, 1992).

In addition, this act also required the FAA to follow the technological developments of security measures. In addition, strict luggage matching application began to be implemented in the airports of the U.S.A. corresponding to this Act in order not to repeat the same tragedy as the one Lockerbie. Congress also ordered FAA to make background check for security personnel and screen passenger luggage with explosive detection technology by 1993. In addition, FAA was responsible for supervising the security managers at the airports whether they were sufficient enough to implement security measures at the airport designed by FAA (Dempsey, 2003a).

The Commission on Aviation Safety and Security – The Federal Aviation Reauthorization Act of 1996

Although all these efforts had been made to improve security, the disaster of TWA Flight 800 could not have been prevented. In 1996, TWA 800 Boeing 747 exploded over the Atlantic Ocean, killing 230 people on the plane. The route of the plane was from New York to Paris. In spite of the fact that evidence showed that a spark in the tank caused the plane to explode, there were some claims that a terrorist bomb caused the explosion (Birkland, 2004). This attack via aviation brought new debates about aviation security. As a result of these arguments, President Clinton summoned a White House Commission whose chairman was Vice-President Al Gore (Rhee, 2000).

The Commission on Aviation Safety and Security, which was also known as the Gore Commission for its chairman, was initiated by President Clinton in 1996. The focus of this commission was to assess and recommend safety and security measures for airports and airplanes. The commission also focused on the danger of explosives on aircraft due to the fact that explosions resulted in more deaths then any other terrorist or criminal activities. New technological developments regarding surveillance and screening were evaluated by the commission, and new policies were developed to determine how to use these technological devices effectively. In addition, new regulations and agreements for security and safety were held between aviation companies and the government (Rhee, 2000). According to this act, security measures had to be improved and considered as an important part of national security (Thomas, 2003). By doing so, in one sense, this commission aimed to respond to all vulnerabilities of aviation security. The Federal Aviation Reauthorization Act of 1996 was enacted to implement the decisions of the Gore Commission. This act ordered the FAA to certify the aviation companies which performed these regulations. It also required the FAA to make vulnerability assessment of airports and airplanes in the United States (Dempsey, 2003a).

However, some implementation problems occurred while the decisions of the Gore Commission were being carried out. These problems in turn caused one of the biggest tragedies in American history, the September 11 attack. As it is in reality, nobody could have predicted whether the attack of September 11 could have been prevented, but the only thing which was apparent was that some recommendations of Commission on Aviation Safety and Security of 1996 were not applied properly. Just a few of the 31 recommendations had been implemented prior to 11 September 2001, including more complicated profiling, passenger-bag matching, enhanced background checks for screeners and airport employees, and cargo threats (Szyliowicz, 2004).

The Omnibus Consolidated Appropriations Act of 1997

The Omnibus Consolidated Appropriations Act of 1997, which provided funding corresponding to recommendations of The Commission on Aviation Safety and Security, was enacted to solve screening security problems by allocating money to FAA. Congress, referring to this act, granted the FAA $144 million to enhance the security screening systems at the airports (GAO, 2004).

According to this act, government was planning to set up 54 explosive detection systems and 489 trace detection devices to screen carry-on luggage at the airports of the United States by 1987. However, just 13 explosive detection systems and 125 trace detection system could be deployed by 1998 by the FAA. In 2001, there were 161 explosive detection systems at the airports. In addition, the FAA analyzed the detections machines to determine whether they were capable of screening for selected explosives. One of the machines that passed their test was the CTX-5000 luggage scanners that had capacity of screen 225 bags an hour (Dempsey, 2003a; Rhee, 2000).

Computer-Assisted Passenger Prescreening Program (CAPPS I)

The Commission on Aviation Safety and Security recommended establishing a national database comprising passenger travel information. Therefore, in 1998, the first computer-assisted passenger prescreening program (CAPPS) was put into practice by the FAA. This program created a target profiling based on passenger's travel information and checked the passenger's payment information and Point of No Returns (PNR). If any passenger fits this profiling, he or she will be investigated at the airports as a potential threat. It also included a detailed security investigation of some people who were selected randomly from all ticketed passengers. Not only the selected people themselves, but also their belongings and carryon were checked (Staff 3, 2003).

However, CAPPS I program, disappointingly, failed on September 11. Although 9 of 19 terrorists were selected by this system, none of them was prevented from boarding the airplanes. Just two of the terrorists were investigated in detail for their luggage, but security personnel found nothing. This failure triggered the TSA to redesign this program under the same name (GAO, 2003).

Aviation Security Improvement Act of 2000

The Aviation Security Improvement Act of 2000 required fingerprinting and background checks of airport and airline security employees in specific airports that were significant in terms of national security (Dempsey, 2003a).

In the past, screening operations were conducted by security companies under contract with a responsible air carrier. There was no information sharing between these screeners and law enforcement and intelligence agencies. The Anti-Terrorism Bill of 2001 pointed out this problem for aviation security to the agencies (Bailey, 2002).

Before September 11, no airplane carrying a US flag had been bombed or hijacked for a decade. On September 10, aviation security stood at a peacetime condition. People were just concerned about delays and overcrowding, and they used to be impatient to keep moving. On September 10, aviation security required balancing the requirements of all segments of aviation in terms of security. After that day, other concerns became more important due to the massive attack. The thing that different governments learned from that massive attack is that aviation security should be responsive to the threat based on information from intelligence and law enforcement agencies.

Before September 11, the US Congress paid more attention to passenger rights. Due to lobbies by the big airlines, Congress pressured the FAA to use more “soft” security policies against airlines and the aviation industry (Thomas, 2003). The FAA also focused on safety, customer service, capacity and economic issues.

The Aviation Industry was also suffering from economic problems, so The Airline Deregulation Act, enacted in 1978, aimed at reactivating the aviation market by offering a competitive environment. According to the experts, the aviation industry in the USA was spending enough money, but much of it was going to address the problems (Sweet, 2002).

Moreover, aviation industry had problems for insufficient security personnel some of whom had difficulties to speak English. In addition, they, mostly, were minimum wage workers and most of them were not trained adequately to screen baggage and passengers competently (Russell & Preston, 2004).

Regulations at the International Level

The first international flight was provided by Lufthansa's airship, Zeppelins, in 1920. This international service covered transportation from Frankfurt to New York and Rio de Janeiro with the world’s largest airship, the Hindenburg. However, as an indicator of future attacks via aviation, this international transportation attempt was terminated by a bomb explosion in 1937 in New Jersey. This explosion, which has been kept secret until recently, killed thirty-six people including the crewmen of the airship and the bomber. Like many other terrorist attacks, officials and executives were informed about the planned bomb attack on the Hindenburg beforehand, but the precautions that they took failed to prevent the catastrophe (Rhee, 2000). After this event, countries began to consider this issue internationally and some countries organized conventions and conferences to stop international terrorist and criminal activities.

Chicago Convention of 1944

After World War II, the Chicago Convention of 1944 was organized with fifty-four nations attending when the United Nations was about to be established. It prohibited the improper use of civil aviation. As an implementation of this policy, International Civil Aviation Organization (ICAO) was established under the United Nations and headquartered in Canada to solve international problems of aviation. The Chicago Convention authorized the ICAO to regulate legislative and technical issues of international civil aviation (Dempsey, 2003a).

In Chicago Convention, the nations attending this convention compromised about two provisions pertaining to international flight. The first provision was the right to fly through another country without landing, and the other was the right to land another country to provide oil or repairs without boarding and leaving passenger or cargo. Generally, in this convention, economic and security issues were the main concerns, so ICAO was assigned to maintain security standards internationally, such as aircraft licensing, airworthiness certification, registration of aircraft, international operating standards, and airways and communications controls (Dempsey, 2003a; Reser, 1998).

Tokyo Convention of 1963

Between 1949 and 1985, 779 hijack attempts were done by terrorists and criminals, but they failed 281 times. Interestingly, in 1960, twenty eight out of thirty hijacking attempts around the world were committed against American aircrafts. In 1963, Tokyo Convention was organized by the international aviation community to evaluate and stop this hijacking trend (Rhee, 2000). This act is considered the first international effort to stop hijacking in the world. It prohibited any unlawful act that would put the airplane in danger during flight. However, the Tokyo Convention had some deficiencies and did not satisfy attending nations because this act did not regulate extradition and prosecution issues, which constitute one of the major problems of international illegal activities (Dempsey, 2003a).

Hague Convention of 1970

Seven years after the Tokyo Convention was held, another treaty, the Convention for the Suppression of Unlawful Seizure of Aircraft, which is also known as the Hague Convention, was signed in 1970 among ten countries seriously concerned about the increase of unlawful seizures of civil aircrafts. Basically, this treaty aimed to fill the gaps of the Tokyo Convention concerning extradition and prosecution of hijackers. This act redefined hijacking as a serious and unlawful act in the air. It required the nations that captured the hijackers to punish them severely. Because of the fact that each country had different prosecution and punishment systems, this requirement was never effective in terms of creating a common punishment for the offenders. It also rearranged the jurisdiction problems regarding where the defendant was prosecuted and where the trial was held. This convention was also criticized because it did not clarify all the circumstances that might happen during an unlawful act (Dempsey, 2003a).

Montreal Convention of 1971

Another treaty, the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation was signed in 1971 to fight against aviation sabotage, like bombings of airports and airplanes. For this reason, this Convention was also known as “Sabotage Convention” or “Montreal Convention” in honor of the place where the conference was held. This treaty was signed by 128 countries and aimed to prevent aviation sabotage around the globe (Rhee, 2000). The reason for making this convention was a general trend in sabotage that was inversely proportional to the decrease in hijacking incidents.

In 1974, the International Civil Aviation Organization (ICAO) enacted Annex 17. In this legislative arrangement, not only were the Tokyo, Hague, and Montreal Conventions incorporated, but also it required each one of the member states to establish an institution that regulated aviation security and set up a security program which included screening, checking process, and training for airport employees (Dempsey, 2003a).

Later in 1978, during the G-7 Summit, member countries signed the Bonn Agreement to fight against aviation-related terrorism. This agreement addressed proscribing flights against countries that supported the aviation-related terrorism and refused to prosecute these terrorists properly or send them back to the country whose airplane was hijacked or bombed (Sweet, 2002).

Tokyo Summit of 1986

In 1986, a similar agreement, the Tokyo Summit, was organized after these conventions by seven countries. The aim of the summit was to fight against terrorist activities and countries that supported these activities. The decisions of this summit included some restrictions and limitations for countries that had any relationship with the terrorist organizations.

In order to provide international cooperation, the ICAO also organized some meetings among countries at different times, one of which was held in 1990. According to this treaty, countries agreed to try to control the proliferation of undetectable and unmarked plastic explosives. To achieve similar goals, a new conference was held in Lyon, Paris in 1996 by security ministers from many countries. They focused on the effectiveness of satellites to determine where the terrorists were. In addition, they made an agreement that each individual country would develop counter-terrorism programs to fight aviation related terrorism (Dempsey, 2003a; Sweet, 2002).

International Convention for the Suppression of the Financing of Terrorism in 1999

In 1999, the International Convention for the Suppression of the Financing of Terrorism was held to prevent terrorist activities by taking steps financially. One of the conspicuous sections of this treaty was that it covered many crimes from drug smuggling to arms smuggling.

Among all these international legislative efforts, the regulations of the ICAO have played the most important role for the aviation sector since its establishment. The ICAO requires its member countries to take necessary precautions for effective aviation security, and it is responsible for standardizing the process of aviation security among 180 member countries. However, in general, all these international regulations have failed to provide effective cooperation between countries to prevent terrorists and criminal attacks against the aviation sector. All these efforts were only relatively successful when they were put into practice. As a result, different countries continued to hold one convention after another. Different evaluations of these convention statements cause different policies and problems among the countries (Sweet, 2002).

Aviation Security Policies in the USA after September 11

On September 11, 2001, four airplanes whose flags belonged to the U.S.A were hijacked in the morning by nineteen terrorists with box cutters. The terrorists managed to occupy the planes and changed their original routes. Two of them, American Airlines Flight 11 and United Airlines Flight 175, were used as missiles to crash into World Trade Center, which had economic and also symbolic significance for the U.S.A and city of the New York. The crash caused the two buildings to collapse due to the large amount of fuel and the effect of the crash. American Airlines Flight 77 was similarly manipulated and crashed into the Pentagon, which is the highest military headquarters of the United

States. The fourth airplane, United Airlines Flight 93, crashed in a rural area of Pennsylvania. This plane was original intended to crash into White House according to some experts (Dempsey, 2003a).

Many new pieces of legislation and policies after September 11 stemmed from the past policy-making practices which were formed after the TWA 800 crash in1986 and the PAA 103 crash in 1996 (Birkland, 2004). However, these regulations were not sufficient to prevent the tragedy of September 11. After September 11, people realized that contrary to previous belief, the transportation security barrier in the United States is easily suppressed. In spite of the fact that intelligence sources had been informed that such an attack might occur in the United States, most people in this country, including many high ranking executives, were completely unprepared it. Terrorists with box cutters managed to get in the airplanes, hijack four of the airplanes, use them as missiles, and kill more than three thousand people (Dempsey, 2003a).

Immediately after the attacks, Congress gave authority to the President to spend $3 million for urgent needs (Thomas, 2003). Except for military jets that patrolled the sky, the entire U.S. aviation system was shut down for three days for the first time in American history. Overall, the numbers of flights in the USA were reduced by 30-35% in the days and weeks following 9/ 11 (Bailey, 2002).

Air Transportation Safety and System Stabilization Act of 2001

"Air Transportation Safety and System Stabilization Act" was promulgated eleven days after the attack. It included grants to the aviation industry, which was really affected by this detrimental event, victim compensation, and some relief for the insurance companies. It required that the federal government take all responsibility and pay the cost of the damages (Thomas, 2003). The driving force of this act was not to address aviation security directly, but rather to prevent the collapse of the aviation sector (Dempsey, 2003a). The other reason for this act was that most aviation companies had to substantially reduce their number of flights, and therefore, had to dismiss many employees (Sweet, 2002).

According to this act, economic assistance came to the aviation sector by different means. These means were direct grants, loans, and a limitation of carrier liability for the crashes that happened on September 11, and federal war risk insurance for the industry. The government granted $15 million to the aviation companies and reduced the liability for two airline companies, the United Airlines and American Airlines, as a requirement of this act.

Moreover, the September 11 Compensation Fund was established to deal with claims for more than three thousand dead (Dempsey, 2003a). After September 11, one of the main concerns that the government dealt with was victim compensation. The main goal of this fund was to help victims of the September 11 attacks. ATSA also regulated the scope of the Victim Compensation Fund by providing compensation to the physically injured victims or relatives of people killed due to September 11 terrorist attack.

Basically, the U.S. Government gave money, a minimum of $250,000 without tax, as compensation to the victims or beneficiaries of those who died on September

11. The beneficiaries had to submit their claims by December 22, 2003. 7,298 beneficiaries applied to get compensation. However, the government put some limitations on who would benefit. One of these limitations was people's eligibility for getting a claim. It made restrictions based on whether physical harm stemmed from the attack or not and if the injury or death happened immediately or in the aftermath the attack. The other important limitation was that if the victims or relatives of the dead took the compensation, they waived their rights to litigate the government for this terrorist attack (Balahadia, 2003).

Aviation and Transportation Security Act (ATSA) of 2001

Aviation and Transportation Security Act (ATSA) was enacted in 2001 to regain the public's confidence in flying on American's carriers. By this law, the duty of aviation security was taken away from the FAA and given to the newly established agency, the Transportation Security Administration (TSA) (Campbell, 2002). Later, as a result of the Homeland Security Act of 2002, TSA was transferred from the Department of Transportation (DOT) to Department of Homeland Security (DHS) on March 1, 2002 (GAO, 2004).

Thus, aviation security was the direct responsibility of the federal government, which included 22 agencies and 170,000 employees. The TSA was given most of the aviation security duties which had previously been performed by the Federal Aviation Administration (FAA) (Dempsey, 2003a). However, the security mission of the FAA was not terminated when the Aviation and Transportation Security Act was enacted. The

FAA was still responsible for air traffic security, the safety and integrity of the aircrafts, and flight crew training (Garvey, 2002). After obtaining the responsibility, TSA took many precautions and measures arising from the act of ATSA, to prevent airports from being a target for terrorist and criminals. These precautions and measures can be examined in several categories.

First, procedural regulations were made. Procedures to increase the screening of passengers before boarding and controlling them through secure areas in the airports are important parts of this Security Act (Campbell, 2002). Generally, airport security personnel screen 1.3 million luggages yearly in airports in the US (Dempsey, 2003a). According to this act, all passengers including their carry-on luggage on the commercial airlines have to pass through security checkpoints (GAO, 2004). For this reason, by using different means, such as exclusive detection machines, physical searches, dog sniffing, and matching bags with passengers, all passengers and cargo can be screened as a requirement of the ATSA. In addition, Congress ordered the TSA to screen all bags including carry-ons, luggage, and cargos until a specific deadline after September 11 (Dempsey, 2003a).

The TSA continued to implement the layered security system at the airports. It created a system with many layers of defense so that terrorists could be deterred and checked at each layer (Thomas, 2003). Layered security system consists of seven different steps of defense; Intelligence, passenger prescreening, airport access control, passenger, checkpoint screening, passenger checked baggage screening, cargo screening, and, on-board security (The aviation security, 2003). These precautions included gathering intelligence for aviation security, then passenger prescreening, passenger checkpoint screening, baggage screening, cargo screening, and on-board security. These layers served to prevent any threats and terrorist activities in the airports (Dempsey, 2003a). In 2003, TSA began to apply a new application at the airports to positively identify individuals with access to secure airport areas by using biometric screening procedures, such as taking fingerprints and photographs (Elias, 2003).

TSA also assisted some airports in improving perimeter and area control security by giving funds for security equipment to them. For instance, electronic surveillance systems were deployed at most airports (GAO, 2004). Briefly, this security system aimed to keep terrorists away from aviation buildings in different passages and divisions, for instance, keeping them away from airports, from airplanes, and from cockpits (Garvey, 2002).

Second, changes in equipment and technology at airports were made. The TSA was ordered to focus on research and development and to organize new security devices and programs for the airports, coordinate intelligence sharing with other agencies, and address the threats against the aviation sector. By doing so, most security functions and units under FAA authority were transferred to the TSA (Thomas, 2003). The condition of all aviation units has been improved. $17 billion has been spent for these arrangements, new technological devices, and screeners. To detect the risky materials and objects, the technologies provided by TSA for screening air cargo include x-ray screening, x-ray based explosive detection systems, chemical trace detection systems, and technologies based on neutron beams. In addition to these technological machines, TSA also aspires to screen cargo by using dogs (Elias, 2003).

The Aviation and Transportation Security Act also required strengthening cockpit doors and installation of video monitors and warning switches on U.S. airlines. Respectively, the rationale for this requirement was to prevent terrorist and criminals from gaining access to the cockpit. It was also to give the cockpit crew the ability to monitor inside the cabin and to be alerted by cabin crew of trouble. In addition, the explosive detection system or EDS, used to scan all luggage, were installed in all U.S. airports (Dempsey, 2003a).

On the agenda of the TSA, there are some plans to increase security by utilizing the new technologies. Biometrics access control identification systems, such as fingerprints or iris scans, anti-piggybacking technologies to prevent more than one worker from entering a secure area at a time, and video monitoring systems for perimeter security are just a few examples which have been evaluated by the TSA (GAO, 2004).

Third, personnel regulations were made. The entire workforce of screeners has been federalized due to the requirement of the ATSA. Moreover, more than 55,000 new workers have been hired (Szyliowicz, 2004). 750,000 airport employees were given a criminal background check and 28,000 prior screeners became federal employees (Dempsey, 2003a). TSA replaced poorly paid, inadequately trained, and inefficient personnel who were provided by private companies in the passenger screening section at the airports with federal employers (Szyliowicz, 2004).

The TSA also hired security personnel or air marshals, who can use lethal weapons, to protect the airplanes from terrorists (Szyliowicz, 2004). Not only did TSA hire air marshals for security, but it also trained them. All air marshals have been trained with a basic and 4 week-advance course operated by the TSA (GAO, 2003).

This act required all airline flight crews including pilots to take training courses on how to deal with terrorists who try to gain control of the aircraft. In addition, Arming Pilots against Terrorism Act of 2002 also permitted the pilots to carry weapons in the cockpit and use them if they face terrorists or criminals who pose a threat and danger to the airplane and passengers.

Transportation Security Administration is also planning to take some additional measures. These include providing a 911 call capacity for all airplanes, designing new ID system for law officers who carry a gun onto the airplane, providing more confident traveler programs, providing constant communication between airplane and ground crew in emergency situations, designing new pilot licenses with biometric features, and using voice biometric technology for screening. Similarly, according to the 9/11 Commission, every cargo airplane has to have a tough container for any suspicious cargo (Levine, 2004).

The results of all implementations of TSA one year after September 11 were quite remarkable. By screening the passengers, they seized 5 million items including 1.4 million knives, 1,101 guns, 15,666 cudgels, approximately 40,000 box cutters, and similar items (Szyliowicz, 2004).

Computer-Assisted Passenger Prescreening Program (CAPPS)-II

The TSA began a new, revised program, which was initiated first in 1998 by the FAA, the Computer Assisted Passenger Prescreening (CAPPS II). The goal was to control passengers whether they pose a risk or not (Levine, 2004). The TSA improved the security conditions in the airports by increasing patrols on and around airports, increasing terminal inspections, using trained dog teams, allowing only ticketed passengers and authorized individuals beyond screening checkpoints, and constituting a zero tolerance policy at all secured areas in the airports. In addition to these measures, TSA has discontinued off-airport check-in (Sweet, 2002).

The CAPPS II system involves prescreening the passengers at two different checkpoints, which is a basic difference from the first program. It is a kind of layered system that controls the passengers at different points respectively in order to reduce the risk of missing possible terrorists or criminals. The main goal of the program is not solely to capture the terrorists or criminals but more to deter them from challenging the security system. As a matter of fact, deterrence is the fundamental tool to cease crime and terrorism (Ravid, 2004). The system is also supported by continuously changing intelligence information to prevent potential terrorist or criminal events from being overlooked. In addition, one of the basic features of the system is to focus more on the prescreening phase outside the airports in order to reduce long lines at the airports.

According to the CAPPS II program, all passengers' information, including their names, addresses, and telephone numbers is required to be given to the TSA before they are issued boarding passes by airline personnel who are in charge to this issue.

After obtaining this information, TSA verifies and checks these names and addresses with the databases of the other law enforcement, intelligence, and aviation agencies. The first check is initiated for whether the obtained names match any terrorists' names on the watch list. Secondly, the criminal and credit checks are held correspondingly. Thirdly, the itineraries and how they paid for their tickets are analyzed. Thus, the TSA can determine whether that particular passenger poses a risk for aviation security before he is even screened of the gates. This system allows TSA to direct its efforts to the real suspects (Rochow, 2004).

Ravid asserts that this system, contrary to the vast majority of claims, is not based on ethnic profiling but rather based on behavioral characteristics since it takes into consideration such behaviors as people's itineraries and lodging preferences (2004). Similarly, Rochow (2004) stated that the goal of the TSA is to enhance the aviation security and provide fast passenger flow. However, it is true that CAPPS II program has changed the perception that everybody has an equal chance of being selected for detailed investigation at the airports.

USA Patriot Act of 2001

The Patriot Act was enacted immediately following the weeks of September 11 to combat terrorism in the United States. Basically, this act extended investigative power of law enforcement agencies in terror cases. It also covered intelligence sharing in the context of terrorism, which is an important part of aviation security. It made it easier for law enforcement agencies to survey and search for terror suspects. However, civil liberties groups have attacked this act because they claimed that this act limited people's personal rights, guaranteed by the American constitution (Carol, 2005).

In terms of aviation security, some people may be obliged to travel with an airplane due to their ethic backgrounds, religions, or race by the security authority referring to this act. This act also allowed the government to collect information from passengers who are flagged as a threat (Dempsey, 2003a).

Homeland Security Act of 2002

The Department of Homeland Security, a new executive agency that was designed to coordinate many existing federal agencies including the Transportation Security Administration, was established in accordance with this act. Twenty-two agencies were joined under the authority of the Department of Homeland Security, whose budget reached $40 billion. Before September 11, no serious domestic terrorist attack had happened on U.S. soil, so there was no need to establish such an agency. By creating this highly authoritative agency, the government's intent was to prevent any more terrorist attacks on the United States, decrease the vulnerability of the security system, and restore the systems after any future terrorist attacks. Its mission was to take maximum precautions against any kind of terrorist attack, such as biological, radiological, chemical or nuclear, by managing all the possible risks. One of the reasons why the government established such a structure was the vast amount of international commerce.

The Department of Homeland Security was required to handle this huge traffic happening at the borders of this country. Typically, each year, 500 million people, more than 11 million trucks, 51,000 foreign ships, and 2.2 million rail cars pass through the borders of the United States. Moreover, the Department of Homeland Security extended the requirements of the Transportation Security Administration in terms of training the personnel, screening the bags and cargo by Explosive Detection System (EDS) technology, and tracking technology for security (Dempsey, 2003a).

Air Cargo Security Act of 2003

The U.S. Senate enacted the Air Cargo Security Act on May 8, 2003 as a regulation like many others after September 11. This act required the security personnel to screen all cargo before placing them onto passenger planes and it also extended the “known shipper” program, which gives privilege to shippers who had previous dealings with the airlines. In addition, this act also necessitates the TSA to inspect air shipping facilities, create an industry-wide database of cargo shippers, and produce a security training program for air cargo managers. The driving force of this act was to ensure the security of all cargo transported in an aircraft operated by either domestic carriers or foreign carriers. This act also involves the Federal Flight Deck Officer Program, which permits air cargo pilots to carry guns like pilots on passenger airlines.

Known Shipper Program regulates the different procedures between known shippers who have had previous business dealings or are known by the air cargo carriers and the shippers who have not done business via air cargo before. The program requires additional procedures and requirements for the new shippers. TSA prohibited the transportation the cargo and mail whose source is unknown (Elias, 2003).

Regulations Made in Accordance with September 11 Commission Report

According to the United States Government Accountability Office (2005), the Transportation Security Administration also had to develop a new passenger-prescreening program, called Secure Flight. The Secure Flight Program allowed the TSA take over from private aviation companies the responsibility for comparing the names on the passenger list with different agencies' watch lists. The driving force of this Secure Flight Program stems from 9 /11 Commission Report which indicated that the watch list used by the commercial airlines did not cover all terrorist' names and was not updated regularly. Moreover, agencies do not want to share intelligence with private companies and other countries. Therefore, TSA was assigned to compare the passenger list and watch list to detect any terrorist's names. TSA expects that this program would not only improve passenger prescreening, but also prevent victimization based on false matching (GAO, 2005).

The Intelligence Reform and Terrorism Prevention Act was enacted in 2004 to improve national security along with transportation security in the U.S.A. by reforming the intelligence allocating process in the United States. It required a change in the organizational structure of the intelligence community to protect the aviation system from terrorist attacks. By enacting this act, the U.S. Congress extended the Aviation and Transportation Security Act (ATSA) of 2001.

Evaluation of Pre- and Post-September 11 Policies in the United States

Since its inception, there have always been concerns and debates over the issue of whether the legislative regulations or policy implementations presented are sufficient to respond to the risks of aviation security. Some people insist that these regulations have handled and resolved many security problems in the aviation sector, but others take a different position and say that most of these regulations either have had many deficiencies or have fallen on deaf ears and not implemented.

In this section, based on literature review of this subject, aviation security policies are evaluated into two parts, pre and post September, to indicate the consequences of those policies and regulations.

Pre-September 11

Generally, most policies that put into practice before September 11 were reactive in nature. They were prepared after a serious terrorist or criminal attack which happened either in the world or in the U.S. (Dempsey, 2003a). Before September 11, the Department of Transportation which was in charge of aviation security, regulated security systems at the airports and airplanes in the United States by dealing with the all vulnerabilities and threats in the system. Screening passengers and cargo by technological devices, helping other nations to improve their security systems, and training the employee were a few examples of what had been done before September 11. The main structure of the security was based on a layered security system. The proponents of this plan believed that this system perfectly addressed risk management issues and would reduce the risks in the system.

However, September 11 indicated that there were many problems and flows associated with each layer in this system. For instance, before September 11, there were only a few countries, such as Canada, Bermuda, and the U.S.A. which dealt with the aviation security by using security guards. Many other countries in the world used law enforcement agencies to handle airport and airplane security. Moreover, in the United States, due to the deregulation of the aviation industry, aviation companies hired security personnel by bidding. Generally, the cheapest provider won the proposal as a result of bidding, which meant less skillful employees worked at the airports. According to its own investigation of the DOT, during 1998 and 1999, illegal access to secure areas of the airport occurred 68% of the time, and in 1999-2000, this illegal access happened 30% of the time. The U.S. General Accounting Office found that screeners of the airport failed to find dangerous objects 13% of the time in 1978, and 20% of the time in 1987 (Dempsey, 2003a).

In pre-September 11 term, the Federal Aviation Association also failed to implement the decisions and requirements of both international conventions and the U.S. Congress. For instance, installing Exclusive Detection Systems (EDS) were not set up at the airports even after the deadline. This agency was criticized for not keeping in step with technology and for being highly a bureaucratic structure. The general belief about the FAA was that it could not manage aviation security professionally; instead, it focused more on aviation safety issues.

Post-September 11

When evaluating the regulations implemented after September 11, there appears to be many unintended consequences of TSA activities. For instance, these security measures have caused inefficiency at the airports. Passengers have to come to airport two hours before their airplanes take-off in order not to miss their planes because they have to wait in long lines at the checkpoints (Thomas, 2003). For aviation companies, these costly and inefficient procedures put them at a competitive disadvantage against foreign carriers (Sweet, 2002). One month after September 11, the highest-ranking aviation security officer, Michael Caravan resigned in protest of the new implementations of security policies (Thomas, 2003).

In the US, long lines or missed flights created chaos in the airports (Levine, 2004). 1,361 flights were delayed as a result of security concerns in only a month in 2001, which resulted in 2,137 hours of flight delay (Dempsey, 2003a). In addition, some people thought that establishing a new agency in the middle of the crisis, which was the heaviest one in the history of aviation, looked like a situation as indicated in this proverb, “Don’t change horses in the midstream.” For instance, the National Guard was assigned to reinforce cockpit doors, but they had no experience with this kind of duty (Thomas, 2003).

Others criticisms concerned the economic inefficiency of post- September 11 policies. Some interest groups, like the Air Transport Association, claimed that these new regulations were too costly and would be burdensome on the federal government (Birkland, 2004). The government spent between $2.5 billion and $5 billion to set up new security system at the airports and airplanes. The new regulations damaged not only the government but also the aviation industry financially (Dempsey, 2003a). As for air cargo transportation, screening all mail or freight was even more troublesome. Fast shipping options was damaged by doing so, which meant a reduction of income for air carriers (Levine, 2004).

The other criticism of post-September 11 policies is that not only does the new system increase people's frustration, but also it reduces people's perception of having individual personal freedom and privacy (Russell & Preston, 2004). Implementing the security precautions create a dilemma between civil liberties and personal and national security. These security threats lead the government to have a more paternalistic approach because the technology permits the government to be more intrusive into people's lives. People's civil liberties are sometimes taken away when the government establishes passenger profiling, biometric detection systems, and technological screening systems (Rhee, 2000).

Moreover, as Szyliowicz noted, new regulations created a conflict between the government and civil libertarians. Although the government claimed that new technology could ease the requirements and reduce the workload, civil libertarians expressed their concerns about the CAPPS II program, which was newly reviewed and revised by the TSA, owing to the fact that it caused racial, religious, and ethnic discrimination during the selection process (2004).

Abusing civil liberties and human rights by using high technological devices as a result of new regulations may provoke different countries and result in international conflicts. The ATSA requires airlines to provide all passengers' information to U.S Customs for national security. The main goal of gathering information is to fight against terrorist and criminals. In addition to domestic flights, this requirement is also obligatory for foreign airplanes flying to/from the United States. If any foreign aviation company does not provide necessary information to the U.S. Custom within the required time, either they are fined or their landing rights to the U.S. Airports are cancelled. However, some countries, such as countries, which are member of European Union, have developed data protection laws for civil rights. Violation of these data protection laws by the U.S. officials produces disagreement and conflict between European Union and the U.S.A. (Gubitz, 2005).

In addition, the TSA has not adequately focused on resolving the identity-theft issue on the CAPPS II program. In many terrorist activities, terrorist use fake identities either by stealing them from somebody or creating a new one.

By the same token, installing technological devices do not always bring positive and effective results. For instance, after the Pan Am Flight 103 explosion, a new thermal neutron analysis (TNA) machine was installed in 100 main airports of the United States. However, the capability of detection for explosives had not been assessed sufficiently. Likewise, a Computerized Tomography (CT) machine has been criticized by airport executives because of its cost, maintenance difficulties, and inadequate technology (Szyliowicz, 2004).

According to Thomas (2004), not all of the materials successfully seized by the newly trained system could be considered as dangerous materials or weapons. Most of the items were simply packed by inattentive passengers and were not related to terrorist activities.

GAO (2004) claimed that the Federal Air Marshal Program has operational and management problems. Likewise, TSA could not respond to the urgent need for trained employees, and it has still difficulties in hiring, deploying, and training its screeners.

With regard to air cargo security measures, according to the observations of GAO, which was held in 2003, TSA did not have specific long-term goals and performance targets for air cargo security. In addition, it also has not developed specific requirements for the screening of air cargo.   Screeners of cargo were not required to get special courses to recognize suspicious materials and security procedures.

In terms of the precaution that allows pilots can carry guns, TSA announced that pilots could access the guns only in the cockpit and when the cockpit door was closed, causing frustration among pilots. It is clear that not all measures recently implemented in light of September 11 tragedies have proceeded smoothly from the technological, business, or general public point of view. The Department of Homeland Security made the requirements for carrying guns into the aircraft or secured area and if these requirements were met, aircrews could carry a firearm into the cockpit (Campbell, 2002). However, Fraher (2004) claimed that a pilot's desire for carrying guns may be based on different reasons, including the desire to play a hero, personal, fear, and traditional habits. After September 11, the factors of morale, social pressure, and the feelings of revenge have been added to these reasons.

There are also other people who found that these implementations are really exaggerated. They claim that the outcomes of terrorist and criminal attacks are generally small in number and can be underestimated**.** They also asserted that the number of people who are killed as a result of terrorist attack is smaller than the number of people who die in traffic accidents around the world. The exaggerated precautions after September 11 are just what the terrorists want to have happen after their attack in order to spread fear among people. For instance, in the case of shooting down a plane by means of shoulder-launched missiles by terrorists, the resulting atmosphere after the attack would be more devastating than the attacks itself to the aviation industry. Fear may cause the aviation sector to initiate economic bankruptcy (Mueller, 2004).

According to the study made by Sivak and Flannagan (2003), after September 11, the risk of being killed in an airplane intended for use as a missile in the USA was one in 13 million. In addition, David Banks, a risk analyst, asserted that no September 11 case would ever occur in the USA again. It was just a shock due to common belief about hijackers. He added that practical and reasonable approach was not established after the event but rather misallocation of funds was made (as cited in Mueller, 2004).

Summary

Aviation security is a never-ending stream of dilemma for not only people who travel with airplanes, but also policy makers of aviation security. There have always been concerns about security at the airports and airplanes due to terrorist and criminal attacks since inception of aviation. Therefore, governments and policy makers produced and developed many legislations and policies to prevent people these attacks. In order to understand the dimensions of outcomes of these attacks and how vulnerable the aviation industry is, aviation security policies are explained in this chapter in accordance with its chronological order. The tragedy of September 11 is chosen as a reference point, so policies are explained into two parts, pre and post September 11.

Before September 11, regulations were generally reactive in nature and developed after a significant attack against aviation sector. In both international arena and within the U.S., policies addressed similar problems in aviation industry. However, after September 11, many security regulations and polices were redesigned and implemented more seriously. It can be evaluated clearly that, aviation industry is much more secure than before September 11. When examining its weaknesses and strengths, aviation security policies have many problems that should be dealt with.

CHAPTER 5

RECOMMENDATIONS AND CONCLUSION

This chapter addresses the risk management phase of risk assessment, avoidance, mitigation, transfer, and acceptance. By indicating these four means specifically for each one of the recommendations, an attempt is made to point out components of successful aviation security by referring those means. Final section of this study is the conclusion.

Recommendations

Components of successful aviation security are products of determining the appropriate solutions to manage the risks in the aviation sector. In this study, by using mitigation and acceptance forms of risk management, some possible strategies are presented to reduce the impact of risks by accepting inherent and substantial risks in aviation security. Similarly, by using means of transfer, the possible risks can be reduced by dividing and sharing with other organizations. As for avoidance, the risk hardening provides to avoid the possible consequences of attacks against aviation. All remedies presented below can be evaluated as responses of the vulnerabilities of aviation security.

Target Options in Terms of Numbers

As long as civil aviation has a large air traffic network, it seems that the aviation sector will never be completely secure. By accepting this undeniable truth, some countermeasures should be developed accordingly to reduce the risk.

Possible remedies of this vulnerability are using and tracking high technology which has always been on the agenda of aviation and government executives, training all the personnel from screening officers to highest executives in the airports to deal with huge numbers of air clients by serving effective and fast service, and public education. Acquainting people on how to behave during an emergency situation in crowded places can be a solution to minimize the risk. This education can be supplied by utilizing the media including the Internet or providing necessary education programs in schools or other educational places. Similarly, if people were not trained and educated properly about how to react during attacks and in what ways they can help officers, the damage would be bigger (Thomas, 2003).

Like all security organization, aviation security is composed of two important components that strongly related each other. These components are human being and hardware including technological detection devices, metal detectors, and x-ray machines. Successful aviation security can not be obtained unless both factors work together properly. Typically, hardware is related to money and technology. Today, any country can purchase the latest technological devices to protect their airports and airplanes on the condition of paying their costs. However, human factor is more complicated than hardware. It consists of people from the personnel who operate the machines at the gates to highest manager of aviation security (Miller, 1993). Training is always perceived as the best solution for the employee in security, but other factors, such as motivation, integrity, and diligence, should not be underestimated. While training personnel, other education methods, such as Neuro-Linguistic Programming (NLP) can be used for security employee to provide motivation continuously. In addition, because of the fact that they always confront with huge number people at the airports, they can be trained about human behaviors and physiology. The courses that the security personnel are trained may also include both physical, such as self-defense and situation awareness courses, and technical programs (Eleven-point, 2004).

Both successful airport management and technological devices can provide systematic order at the airports. Not only does this situation prevent airports from becoming chaotic and disorderly, which the terrorist highly desire, but also it creates effectiveness for this service by reducing long lines that cause delays at the airports. However, while minimizing the risk, effectiveness should be taken into account. In today's world, where rapid commerce has become the norm, these systems should be effective in addition to being secure. Businessmen, especially, do not want to wait at the airports for hours. For this reason, both government and private aviation companies should work together against terrorists to take necessary precautions in both airplanes and airports (A must do list, 2001).

Lack of International Security Standards

Notably, after the tragic impact of aerial crimes surfaced and began to affect other countries either directly or indirectly, people realized that some preventive precautions must be taken to fight this crime immediately by cooperating with other nations. However, no precautions have been taken internationally (Wilkinson & Jenkins, 1998). Based on this reality, it is clear that there should be a global policy that transfer and mitigate the risk in international aviation security. Moreover, by using risk hardening means, all governments should enhance their security system to save people's lives and money.

Aviation security should be considered and evaluated at the international level as well as a national level. Even if some countries succeeded in deterring attacks against the aviation sector, foreign airlines could be used for terrorist and criminal attacks. After September 11, many criteria and legislative actions have been taken by many countries and ICAO, such as the Aviation Security Plan of Action which regulates the ICAO's security standards (Szyliowicz, 2004). The CAPPS II program also obtains data from both American citizens and foreign nationals on international flights that enter the USA, so it is undeniable that this issue needs international cooperation (GAO, 2004). Intelligence sharing and cooperation with other countries are also important factors to prevent any attacks against the aviation industry (Wall, 2004).

Moreover, the founding of an international criminal court is necessary for global aviation security in addition to creating an international standard for prosecution to deter criminals and terrorists. This court should cover not only prosecution issues but also extraditions of the accused terrorists and criminals. After reviewing the risks in aviation sector, the countries that have commercial international flights in the world should seek to achieve mutual self-interest by securing international harmony in law (Dempsey, 2003a).

On the other hand, standardization of security measure of aviation is not easy due to the fact that security measures require considerable labor force and are also capital intensive. However, many developing countries experiencing economic trouble may have implementation problems and may not achieve necessary standards as well as the developed countries can. Therefore, the international organizations should consider this side effect of cooperation for poor countries. As a matter of fact, there had been some attempt made before September 11 by the U.S.A. However, more effective and binding applications are needed today (Cobb & Primo, 2003).

Insufficient Security Systems in the Aviation Industry

The avoidance and mitigation of risk management should be implemented in all airports and airplanes. The possible threats that can break the security at the control points should be avoided by establishing effective security devices and hiring trained personnel at the airports. Moreover, the security system should include all regions and sections of the airports and airplanes, including towers, airport terminal buildings, hangars, gas stations, radio broadcasting devices near airports, such as ADF, VOR, runways, lighting system, radar systems, and outside antennas. All these elements of airport are protected by airport perimeter systems to provide risk hardening. This system consists of a physical barrier that is sometimes combined with electronic perimeter security devices. Whichever system is established at the airports, this perimeter security system should be reinforced with additional measures, such as camera, additional lighting, or installing approved barriers due to potential risk they pose (Thomas, 2003).

In terms of internal security system, setting up the latest technological devices is already in the agenda of governments. However, personnel training should also be considered similarly. In this condition, institutional culture plays considerable role. In the training program, these differences among institutional cultures of aviation security employees should be considered. Even if the government spent huge amounts of money for technological devices, all these machines can not work properly unless highly motivated personnel use them. In this regard, programs or back up courses should be organized to increase the personnel's motivations. Therefore, training programs are one of the components of successful aviation security. In addition, in these programs, personnel should be informed that they must pay attention not to make discriminate passengers. They should secure the airports and aircrafts both effectively and at the same time pay attention to human rights (Eleven- point, 2004).

Also, at the airports, an emergency response team, crisis management organization, and evacuation plan must be established in the case of disasters and emergencies.

Along with technological devices, detector dog teams have been used in airports for a long time in order to detect explosives, contrabands, and other illegal materials to gain security at the airports. However, according to Hunter (2002), training and certification of dogs and its handler have not been standardized up to now. Any false alarm may cause significant problems due to sensitive nature of searching regarding privacy of people. Therefore, in all airports, to provide standardization and quality, both dog teams and their handlers should be certificated by the licensed authority.

Vulnerabilities in Cargo

In addition to precautions taken before and after September 11, such as the known "shipper program" which prohibits shipping for an unknown sender, increased cargo inspections, security training program for cargo employees, and increased security control throughout cargo operations, additional regulations for air cargo security should also be taken. For example, packaging of materials should be reevaluated and the companies should provide tamper-resistant package for their cargo which will be shipped by air. In this regard, companies may use tamper-evident tapes providing visual indicator on the package for their cargo (Elias, 2003).

Air cargo managers should be informed about possible risks in air cargo and trained on how to take maximum precautions against threats. If they are properly trained, the standardization for screening air cargo can be established in the airports. They can be more aware of any suspicious activities in their jurisdictions. In this context, cargo employee should also be trained regularly to adapt to new technological developments in screening cargo and to refresh their information about possible risks and threats in the air cargo. Workers should also be checked for their criminal records before they are employed. In the air cargo facilities, accessibility should be rearranged, and also biometric technological devices can be set up at the gates to prevent penetration to the cargo section of airports.

By transferring the risk to other organizations, such as insurance companies and other private cargo firms, the possible risk can be reduced. For instance, the process of transporting cargo requires bilateral cooperation between the federal employees which screen the materials and private companies which transports them on their aircrafts. Therefore, in order not to have disasters stemming from air cargo, both governments and private sectors should work together to secure the cargo transportation systems and share the liability of the possible damage (Szyliowicz, 2004).

Vulnerabilities in Airplanes

To provide avoidance of risk for the airplanes, risk hardening techniques should be applied to them. For instance, every commercial airplane needs a new transponder which is used for measuring the airplane's airspeed, altitude and location. The features of these new transponders would be that they can not be turned off manually and are connected to the ground directly. Today's transponders can be turned off manually. When it is turned off, air traffic controllers cannot follow the plane. Therefore, they suppose that an airplane has either crashed somewhere into the ground or blown up in the air. Moreover, they cannot send emergency rescue teams to save the plane. If it is hijacked, the only thing that they can do is to wait until terrorists contact them.

For these reasons, new transponder seems to be essential for airplane security. In addition, continuous operation and communication by an airplane transponder should be ensured for emergency situations (Campbell, 2002). According to the international aviation rules, code 7500 is used to indicate that the airplane is hijacked. The intent of the new transponders and related rules was to facilitate the emergency activity of pilots who are under risk of death. The FAA has begun the process of developing these new devices that make it impossible for a hijacker to turn them off, which happened on three of the four September 11 flights (Birkland, 2004).

Preventing unauthorized entrance to the cockpit is a major element of security in the planes. This issue is addressed by the Federal Air Marshal Program after September 11 (Garvey, 2002). In every commercial airplane, there should be a strong cockpit door which prevents terrorist from entering to take over the plane. According to the experts, a steel door may do this job properly. In addition, using video monitors that show what is happening in the cabin and passenger section may warn the pilots to take necessary precautions (Campbell, 2002). However, the cockpit door should not be opened during flight. Otherwise, terrorists may take advantage of this situation and may enter the cockpit and close it, so this useful precaution may turn into disadvantage to the aircrew.

To transfer the risk, emergency transmission devices should be used to inform others at the airplanes. For instance, a panic button, which transmits a signal to the air traffic controllers in the event of a hijacking, may also be beneficial during a hijacking of airplane. When this button is activated by pilots, the airplane does not accept a pilot's manual control. It instead automatically connects and responds to the directives from air traffic controllers on the ground (Wall, 2004).

The automatic landing system can be helpful if a terrorist is trying to hijack the aircraft while it is landing. This system allows the aircraft to land itself without a pilot.

Today, all airplanes are landed by pilots because automatic landing system is a little risky when the weather is not clear. Nevertheless, it can be useful for terrorist while the hijacking is in progress.

The other important issue is that all pilots should be trained in defensive flight maneuvers because terrorists can try to damage the structure of the aircraft. This may occur when terrorists cannot enter the cockpit due to the strong steel door, and they might force the plane into an emergency landing. In addition, pilots can observe the inside of the airplane by watching the video cameras and microphones earlier installed earlier (Easterbrook, 2001).

Vulnerabilities in General Aviation

Like many other areas of aviation security, general aviation also needs new regulations and standardization for security concerns to mitigate the risk for them. Accessibility of these airplanes should be restricted. If these planes, such as crop dusters, are operated by private individuals outside the airports their owners should be obliged to have them locked and protected from a third person while they are unused (Szyliowicz, 2004).

In order to prevent misuse of rented airplanes, the regulations designed for commercial and cargo aircrafts, including perimeter controls, prescreening and screening procedure, and security precautions, should also be applied to these rented airplanes. Moreover, background check for people who want to rent an airplane should be made and the names should be checked by Transportation Security Administration (TSA) to determine whether they are on the watch list or not.

Because of the fact that flight schools were used as a method of September 11 attack's terrorists, flight schools should be also inspected regularly for security violations. Security and safety regulations should also be applied to these schools. In addition, similar background checks may be requested for applicants and current students in the flight schools.

Lack of Intelligence Sharing

Intelligence is the first step for defense of a country and basic tactic of avoidance of risk management system. Its strengths and weaknesses affect the vulnerability and deterrence of the defense system in a country that must protect itself against criminals and terrorists. In terms of aviation security, intelligence is needed to prevent any actions against this sector. In the USA, in spite of the fact that the Federal Aviation Administration (FAA) is not a member of the US intelligence community, there is a department in the FAA to gather intelligence for security of aviation (The aviation Security, 2003). Likewise, the Canadian government also supports intelligence agencies in improving aviation security measures for the sake of national security (Wall, 2004).

Similarly, sharing intelligence among agencies, airports, and airlines is a necessary precaution for defense of a country and aviation security. For instance, due to the fact that terrorists may try to gain benefit from workers by intimidating or bribing them, FAA verifies and checks worker's identity and background, controls the passengers from the watch lists, and follows the current threats against aviation industry by coordinating with the FBI, CIA, and the State Department (Garvey, 2002).

After September 11, the international community was urged to admit to the importance of intelligence cooperation in aviation security. Typically, it will be limited and confidential in nature, but it is clear that even a small piece of information may save thousands of lives (Herman, 2002). Many experts believe that the September 11 attack would have been prevented if there had been cooperation between the FBI and the FAA (FAA: A Failure, 2001).

Sharing intelligence has to be made among agencies that are similarly situated, and there should also be vertical cooperation and communication among different levels of agencies to help information flow regularly so that lower level agencies, assigned to implement the rules, can be aware of the possible threats.

Forgery and Deception

In terms of forgery of passports, each country in the world should design the passports that would be harder for forgers to copy to mitigate the risk of being forged. For instance, some countries, such as Canada, have developed smart chip passports with biometric information that provide face recognition system in addition to travel documents to control any threat and danger to the passengers (Wall, 2004).

To prevent forgery and falsification of passports, in addition to adding anti-forgery safeguard features on passports, there needs to be a study that determines which country in the world has passports that can be easily forged or without specific protection features. After obtaining a list of these countries, the personnel handling the passports at the airports can be more attentive to the holders of passports from these countries.

As for theft of aviation personnel's uniforms, the security passes with biometric features may be a remedy for this problem. Even if somebody steals a uniform from either pilot or screening employees, the biometric featured entries would prevent this kind of deception (GAO, 2004).

Easy Target for MANPADS

To prevent defenseless airplanes from MANPADS, there are some strategies which were developed and presented to the aviation community in the world to avoid the risk of being attacked of this weapon. First, measures designed to prevent aircrafts from being hit by a MANPADS may be a solution. Increasing patrol around the airports, strengthening the perimeter around the airports by increasing their height, using warning systems against missiles, and using other technical measures like flares that would redirect the direction of the MANPADS are a few examples.

Second, airplanes can also be modified to minimize the damage after being attacked by this weapon. Increasing the numbers of the fire extinguishing system at possible hit points can solve this problem. Third, the most effective way to prevent the damage of this weapon is taking proactive measures. Intelligence agencies should follow possible sellers and terrorist or criminal organizations. They should observe the terrorists to determine if they are intent on initiating this kind of attack against aviation or not. Fourth, like other aviation security measures, international cooperation is required to stop the smuggling of this weapon. Legislative solutions should be enhanced even if some international regulations were made.

In terms of accessibility of information, every institution, which has vulnerabilities against terrorist or criminal activities, should be more attentive to what they post. According to Nickson (2002), companies that deliver or make electricity, natural gas, chemicals, and any jobs which need security protection should be aware of the information they provide on their websites. This information should be screened for any potential misuse against the public or that specific company. Removing the sensitive data from the website is a basic level of risk management for the general community.

Vulnerabilities Aviation Computer Systems

Because of the fact that the aviation industry relies on a computer-based system to accomplish much of its work, all the vulnerabilities of computer system in aviation security necessitate a common cyber strategy which would include not only the government but also private aviation companies. In order to avoid the risk, first of all, by providing a common strategy on a national level, the government can follow the attackers, assess the dimension of threats and distribute the defense strategies to all the institutions and organizations that are vulnerable to cyber terrorism and cyber crimes. Moreover, all the departments may benefit from a kind of early warning system. By using this system, cyber attacks will not affect whole branches of the government (Mann, 2002).

Second, to prevent cyber attacks against aviation security, a basic precaution is to install spy protection software programs into the system. However, in this era of rapid changes in technological world, alternate software programs have continued to be developed by many hackers in the world. Therefore, aviation security managers need to follow technological developments in this sector. In addition, they should cooperate with computer experts and purchase special software programs to protect their databases and communicate with the government and civil aviation companies.

Third, when operating computers, using encryption, authentication, digital signatures, and digital certificates can be solutions to prevent accessibility of important databases in an aviation security system. Therefore limited numbers of people operating the system with their digital signatures are authorized to use them. However, it should be careful about who to authorize to use these digital signatures and how to manipulate them. Still, background check is needed in this area.

Fourth, to maintain system safety, there is a need for system security and reliability to mitigate the risk of being attacked from either terrorists or criminals. Although it is difficult to perform a successful attack via computer systems, and despite having enough countermeasures against this, some similar accidents show that necessary precautions should be taken in this area to maintain reliability continuously.

Fifth, due to the fact that the attacks appear in the form of hacking via the Internet and physical abuse to facilities where the computers are located, there should be both physical security and software security for risk hardening to close down vulnerabilities in these sectors.

Unintended Consequences of Measures

Obviously, it is hard to prevent unintended consequences of these measures, even if they are designed and implemented elaborately and carefully. The possible risk should be accepted and some of error should be estimated into the system while the aviation security policies are being carried out.

However, if the quality controls and inspection to the aviation security units are increased and regulations about security issues are updated regularly, then the defects can be minimized. In addition, risk assessment can be systemized and some experts can be assigned to make risk analysis regularly; the TSA created such a unit under its department (Thomas, 2003).

Under wartime conditions, human rights have always been subordinated by governments. In the United States, because it was declared by the President that the war began after September 11, it is claimed that many regulations of aviation security violated human rights. However, some also claimed that they were not made intentionally. They were just unintended consequences of regulations for aviation security. Whatever the justification, human rights which are supported by the constitution in many countries should not be violated (Dempsey, 2003a).

Similarly, discrimination at the airports due to ethnicity, gender, and social status should be prevented as requirement of both constitution and statutes. Any complaints and claims should be evaluated. In addition, it should be remembered that the best security can only be obtained with the cooperation of community as a whole (Birkland, 2004).

New Forms of Crimes

Like other areas of aviation security measures, risk hardening and risk avoidance techniques should be applied to prevent of happening these crimes via aviation means. In terms of these kinds of crimes, general aviation representatives should be attentive to airplanes being stolen from less secure areas. Otherwise, they may be used as a tool to attack chemical and nuclear plants by terrorists (Thomas, 2003). These airplanes may also be used to poison water sources, agricultural fields, and the general environment to damage a particular country. All precautions that were described in general aviation section would apply to these new forms of crimes (McGrown, 2001).

Threats: Terrorists and Criminals

There have always been the possible risks of terrorists and criminals in the world. There is no system in the world that stops these people’s activities. However, terrorism is the worst activity in the world whatever the form, whoever makes it, and wherever it occurs. People should be aware of how horrible terrorism is and take necessary precautions to mitigate the risk stemming from them. The aviation industry and governments especially have to be one step ahead of terrorists. By taking some precautions, people will become more confident when they fly and terrorists will not be able to impose their political demands and hidden intents on the governments. Therefore, with respect to the tremendous terrorism threat all over the world, it is undoubtedly clear that aviation security policy must be reevaluated.

In today's conditions where terrorism is a dominant issue, criminal activities, such as organized crimes should be prevented while dealing with terrorists. Legislative regulations can be arranged to deter more criminals. By risk hardening the aviation means, criminals should be deterred to choose aviation to carry out their activities, such as smuggling by airplanes and theft at the airports.

Conclusion

In conclusion, as a result of risk assessment of aviation security, it can be claimed undoubtedly that aviation industry has various vulnerabilities and threats in different areas of this sector. Therefore, aviation security should be redesigned in accordance with these risks.

Risk assessment instruments provide us to understand the dimensions of risks. In aviation security, vulnerabilities can be observed in various areas; excessive target options in terms of numbers, lack of international security standards, insufficient security systems in the aviation, vulnerabilities in cargo, airplanes, and general aviation, lack of intelligence sharing and cooperation, forgery and deception problems, being easy target for attacks, vulnerability in computer systems in aviation, unintended consequences of measures, and the dangers stem from new forms of crimes. All these vulnerabilities are threatened by two groups, terrorists and criminals. The impacts of these attacks have always been distressing for people and governments. These impacts, especially, have been observed in the media, the economy, the political arena, and the psyche of people.

Utilizing these vulnerabilities, terrorists and criminals have attacked many times in various ways to aviation sector since its inception. Particularly, the most destructive terrorist attack by means of aviation is the tragedy of September 11, which is also the cornerstone of today's aviation security policies. Before this event, the concerns were generally directed at increasing the quality of service of the aviation industry and trying to solve economic problems from which the aviation industry really suffered. After going through the shock of September 11, new legislations and agencies were established. All security precautions were reconsidered and reassessed.

Notably, to response terrorist and criminal attacks, governments have made many regulations and took a lot of precautions both in international and domestic arena to prevent these attacks stemming from terrorists and criminals. However, because of difficulties in establishing a prefect security system that satisfies everybody, governments had to make many reattempts to solve this problem.

The challenge for aviation security is to provide an uttermost level of protection in a way which maintains the support of private airline companies to keep their schedules. Today, passengers not only demand to be secure, but they also do not want any delay in their travel plans whatever the reason. Moreover, supporters of human rights oppose some implementation of security measures. Hence, policy makers should prepare a policy that covers various factors that not only can the vulnerabilities of aviation security be addressed, but also consider the people's demands and human rights.

Based on risk assessment techniques, this study has depicted general framework of aviation security up to now. However, risk assessment results should be validated regularly due to alteration of conditions. Therefore, this study should be extended in the future in accordance with new situations.

REFERENCES

Abeyratne, R., (2002). Crisis management toward restoring confidence in air transport-legal and commercial issues. *Journal of Air Law and Commerce, 67,* 595.

Altheide, D.L. (2004). Consuming terrorism. *Symbolic Interaction, 27*, 289-308.

A must-do list for commercial aviation*.* (2001). *Aviation Week & Space Technology*, *155*(21), 110.

Auger, R. W., Seymour J. W., and Roberts Jr. W.(2004). Responding to terror: The impact of September 11 on K-12 schools and schools' responses.*Professional School Counseling*, 7.

Bailey, E.E. (2002). Aviation policy: Past and present. *Southern Economic Journal, 69*, 12-21.

Balahadia A. D. (2003) Preparations for a storm: a proposal for managing the litigation stemming from September 11th, 2001. *Pepperdine Dispute Resolution Law Journal, 4*, 61.

Berrick C.A. (2003). Aviation Security. *FDCH Congressional Testimony*.

Birkland, T. A. (2004). Learning and policy improvement after disaster. *American Behavioral Scientist, 48*, 341-364.

Campbell, R. P. (2002). America acts: Swift legislative responses to the September 11 attacks. *Defense Counsel Journal, 69*(2), 139-152.

Carol, W.L. (2005). The clash between security and liberty in the U.S. response to terror. *Public Administration Review, 65*(1), 18-31.

Coates, J.F., (2002). R&D leaders face a post-9/11 world. *Research Technology Management, 45*(3), 7-9.

Cobb R. W., & Primo, D. M. (2003). *The plane truth: Airline crashes, the media and transportation policy.* Washington, DC: Brookings.

Coshall, J. T., (2003). The threat of terrorism as an intervention on international travel flows. *Journal of Travel Research,42*, 4-12.

Coughlin, C. C., Cohen, J. P., and Khan, S. R. (2002). Aviation security and terrorism: A review of the economic issues. *The Federal Reserve Bank of St. Louis,84*(5), 9-24.

Dempsey, P. S., (2003a). Aviation security: The role of law in the war against terrorism. *Columbia Journal of Transnational Law, 41*, 649.

Dempsey, P. S., (2003b) Transportation: A legal history. *Transportation Law Journal,30,* 235.

DHS Raises concern about attacks on chemical plants. (2003). *Chemical Week*, 165(31), 5-11.

Easterbrook, G., (2001). Open door policy*. New Republic, 225*(14), 16-19.

Eidelson, R.J., D'Alessio, G.R., and Eidelson, J.L. (2003). The impact of September 11 on psychologists. *Professional Psychology*, *34*, 2.

Einav, O. (2003). Understanding aviation terrorism. *Interavia*, *58*, 670-704.

Eleven-point plan for U.S. aviation security. (2004). *Aviation Week & Space Technology, 161*, 90.

Elias, B. (2003). Air Cargo Security. *Congressional Research Service.* Retrieved 01/27/2005 from http://www.loc.gov/crsinfo/.

Enz, C. A., & Canina, L. (2002). The best of times, the worst of times: Differences in hotel performance following 9/11. *Cornell Hotel and Restaurant Administration Quarterly, 43*(5), 41-53.

FAA: A failure in aviation security. (2001). *Aviation Week & Space Technology*, *155*(15), 94.

Fraher, A.L., (2004). Flying the friendly skies: Why us commercial airline pilots want to carry guns. *Human Relations, 57*, 573–595.

Friedman, E.A. (2001). Airline antitrust: getting past the oligopoly problem. *University of Miami Business Law Review, 9*, 121.

Garvey, J. F., (2002). The airline industry: Post September 11th. *Vital Speeches of the Day*, *68*(9), 277-281.

General Accounting Office. (2002). *Vulnerabilities and potential improvements for the air cargo system*, 03-344.

General Accounting Office. (2003). *Post-hearing questions related to aviation and port security*. 04-315R.

General Accounting Office. (2004). *Aviation security: Improvement still needed in federal aviation security efforts,* 04-385.

General Accounting Office. (2005). *Measures for testing the impact of using commercial data for the secure flight program,* 05-324.

Ghobrial, A., & Irvin W.A. (2004). Combating air terrorism: some implications to the aviation industry. Journal of Air Transportation, 9(3), 67-87.

Greenberg, M., (2003). The limits of branding: The world trade center, fiscal crisis and the marketing of recovery. International Journal of Urban and Regional Research, 272, 386-416.

Gubitz, A. S. (2005). The U.S. Aviation and Transportation Security Act of 2001 in conflict with the E.U. data protection laws: how much access to airline passenger data does the United States need to combat terrorism? *New England Law Review,* 39, 431.

Hale, D., (2002). A September 11th reflection. *The International Economy, 16*(4), 34-37.

Herman, M., (2002). 11 September: Legitimizing intelligence? *International Relations, 16*(2), 227-241.

Hunter, D. (2002). Establishing a presumption of reliability for detector dog teams used in airports in light of the current terrorist threat. *Dayton Law Review,28*, 89.

Kim, H., & Gu, Z. (2004). Impact of the 9/11 terrorist attacks on the return and risk of airline stocks. *Tourism and Hospitality Research, 5*(2), 150-164.

Kelly, S. S., (2000). Federalism in flight: Preemption doctrine and air crash litigation. *Transportation Law Journal*, *28*, 107.

Levine, S., (2004). Toward safer skies; aviation security has improved since 9/11 but not by enough. *U.S. News & World Report, 137*, 10-42.

Mann, P., (2002). Cyber security `missing' from travel defenses. Aviation Week & Space Technology, 157(2), 41.

Manning, S., (1996). The United States' response to international air safety. *Journal of Air Law and Commerce, 61,* 505.

Miller, A. M., & Heldring, M. (2004). Mental health and primary care in a time of terrorism: Psychological impact of terrorist attacks. Families, Systems, & Health,22(1), 7-31.

Miller, R.R., (1993). The people problem. *Security management, 37*(6), 49-52.

Mueller, J. (2004). A False Sense of Insecurity. Regulation, 27(3), 42-47.

Neumann, P.G. (1997). Computer security in aviation: vulnerabilities, threats, and risks. International Conference on Aviation Safety and Security Reports. Washington DC.

Nickson, S. (2002). Accountability versus security. Risk Management, 49(1), 8.

Nordwall, B. D., (1997) Cyber threats place infrastructure at risk. Aviation Week & Space Technology, 146(27), 51.

Ravich, T. M. (2002). Re-regulation and airline passengers' rights. *Journal of Air Law and Commerce,67*, 935.

Ravid, I., (2004). Safety versus defense: comments on “CAPPS II: the foundation of aviation security?”. *Risk Analysis, 24*, 929-931.

Reser, H. E., (1998). Airline terrorism: the effect of tightened security on the right to travel. *Journal of Air Law and Commerce, 63*, 819.

Rhee, J. L. (2000). Rational and constitutional approaches to airline safety in the face of terrorist threats. *DePaul Law Review*, 49, 847.

Rochow, D. V. (2004). Capps II and the Fourth Amendment: does it fly? *Journal of Air Law and Commerce*, 69. 139.

Russell, P. A., & Preston, F.W. (2004). Airline security after the event. American Behavioral Scientist, 47, 1419-1427

Schwartz, A. R., & Bayer, M. J. (1992). Pan Am Fight 103 and the aviation security improvement act of 1990. *Logistics and Transportation Review, 28*, 61-75.

Skinner, J. (2004). An American Civil Law Respond to International Terror. *Journal of Air Law and Commerce,* 69, 545.

Stamper, J. W. (2002). Looking at the events of September 11: Some effects and implications. *Defense Counsel Journal, 69*(2), 152-169.

Staring, G. S. (2003). Admiralty Law Institute: Confused Seas: Admiralty Law In The Wake Of Terrorism: Insurance And Reinsurance Of Marine Interests In The New Age Of Terrorism. *Tulane Law Review*, 77, 1371.

Sweet, K. M. (2004). *Aviation and Airport Security; terrorism and safety concerns.* New Jersey: Pearson Education.

Szyliowicz, J. (2004). Aviation security: Promise or reality? *Studies in Conflict & Terrorism, 27*(1), 47–63.

The 9/11 Commission Report of the National Commission on Terrorist Attacks Upon the United States (2004). Retrieved 03/15/05 from http://www.gpoaccess.gov/911/

The Aviation Security System and the 9/11 Attacks. (2003). (Staff Statement No. 3). *National Commission on terrorist attacks upon United States.* Retrieved 02/10/2005 from http://www.fas.org/irp/congress/2004_rpt/staff_statement_3.pdf

Thomas, A. R. (2003). *Aviation insecurity*, New York: Prometheus Books.

Wall, R. (2004). More security: Ottawa increases funding for intelligence, maritime patrol. *Aviation Week & Space Technology*, *160*(23), 62.

Wilkinson, P. & Jenkins, B., (1998). Introduction*. Terrorism & Political Violence*, 10.