Airport Security and TSA: A Case Study Analysis

Dissertation Manuscript

Submitted to Northcentral University

School of Business

in Partial Fulfillment of the

Requirements for the Degree of

DOCTOR OF BUSINESS ADMINISTRATION

by

RADOICA NATACIA CLEMENT

La Jolla, California

August 2019

Approval Page

Airport Security and TSA: A Case Study Analysis

By

RADOICA NATACIA CLEMENT

Approved by the Doctoral Committee:

DocuSigned by: Marsha Tongel 5090416D1497485...	Ph.D.	10/10/2019 | 13:08:46 MST
Dissertation Chair: Marsha Tongel	Degree Held	Date
DocuSigned by: Abigail Scheg 792AC842649B4AF...	PhD, MBA	10/15/2019 | 05:38:23 PDT
Committee Member: Abigail Scheg	Degree Held	Date
DocuSigned by: John Bennett 213D7AE93E00403...	Ph.D.	10/10/2019 | 16:05:45 MST
Committee Member: John Bennett	Degree Held	Date

Abstract

Security is an issue of great concern in the transportation sector as terrorists and terrorist tactics are evolving. This dissertation examines how and why the Transportation Security Administration (TSA) chose the current airport security system that is highly criticized by patrons and the aviation industry as being ineffective and inefficient. The purpose of this qualitative single case study is to explore the operations of the TSA in terms of resource allocation and the extent to which it uses or should use a risk-based approach to resource allocation. Using a thematic analysis, this study analyzed past and present secondary data of the TSA's current airport security system. I used secondary data gathered from the Government Accounting Office (GAO), Congressional hearings and the TSA. Overall, 63% of the documents collected discussed elements of the TSA's effectiveness, compared to 32% which discussed inefficiency. However, there was a slightly higher frequency reported of TSA's inefficiency as compared to its effectiveness and efficiency. In conclusion, this study provided insight on how and why TSA chose the current airport security system and the role the GAO, congressional hearings and the TSA itself attributes to the improving the aviation security system. Further studies into both the limitations and the uncovered and unexplored themes of the literature of this study would benefit the field of homeland security and transportation security tremendously.

Acknowledgements

I would like to acknowledge and thank the following important people who have supported me, during the course of my academic journey and my life.

Firstly, thank you God for life and your grace.

I would like to express my heartfelt thanks, to Dr. Tongel, Dr. Walters and Dr. Bennett, without your expertise, encouragement, patience, and guidance I would be lost. To the staff of Northcentral University that has assisted me with technical difficulties, course changes and everything in-between thank you for your patience and assistance.

To my friends and family, who are too many to name, thank you for your understanding, support, encouragement and patience and at times a shoulder to cry on.

Lastly, to the two most important people in my life. To my late sister Portia Clement-Sankar, thank you for teaching me that love may sometimes take the form of sacrifice and grace. To my daddy, Roy Clement, thank you for teaching me to lead by example, and for encouraging my every dream and aspirations be it big (such as pursuing a doctoral degree) or small (such as learning how to ride a bike) is attainable. With all my heart I love you both to the moon and back.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

Security in airports has always been a principal concern, and with the continuous increase of terror threats, there is a great need for vigilance on this issue (Lee & Jacobson, 2012). Several incidents that have occurred in planes and airports across the globe indicate the need for well-organized security measures to avert any form of threats to both people and property, which include hostage-taking, bombings, and physical attacks (McFarlane &Hills, 2013). However, after the terrorist attacks in the United States on September 11, 2001, which left a trail of deaths, casualties, and significant loss of property, there has been a new awakening for airport and flight security on a global scale (McFarlane & Hills, 2013). After the terrorist attacks of September 11, 2001, the U.S. federal government and other world jurisdictions made a quick move to increase budgets for the security of the aviation industry to better control a thorough screening of the people and luggage in the airport facilities (Edwards, 2013). The increased aviation budget was coupled with the rapid formation of the Transport Security Administration (TSA), that would be fully in charge of all the security matters, including screening, at all airport facilities (Edwards, 2013).

The Aviation and Transportation Security Act (ATSA) was enacted two months after the September 11, 2001, terrorist acts (Janic, 2015). According to Poole (2009), the TSA was created to be responsible for the security issues in the transport sector. However, most of the department's budget is channeled to aviation security, specifically to the screening of passengers and luggage (Poole, 2009). Unfortunately, no risk assessments of individual airports were conducted before implementing the new enhanced screening procedures, leading to budget misallocation and waste, particularly when the TSA was placed under the umbrella of the Department of Homeland Security (DHS) (Price & Forest, 2016). The current TSA security

system has been described as inefficient and rigid, whilst attempting to ensure safety (Janic, 2015). Most of the systems that are in place combine multiple resources, such as metal detectors and X-ray machines, for detection of metallic and electronic materials that can be harmful (Janic, 2015).

Almost two decades after the creation of the TSA, audits on the performance of its screening program indicate that it is less effective than private screening because of the inefficiencies and overly bureaucratic processes (Edwards, 2013). According to Price and Forest (2016), the TSA has also been under scrutiny for mismanagement, security failures, and suspicious investments. There have been numerous public accounts of the TSA unnecessarily targeting certain demographic groups, such as individuals who are of Middle Eastern decent. Some researchers suggest that the current aviation security system does not utilize resources efficiently and is not strategic in dealing with the ever-changing threat situation of the contemporary world, making the TSA ineffective for use in the aviation industry of this age (Price & Forest, 2016).

Some researchers also suggested that the TSA does not take into account the variations in infrastructure and access points from one airport to another (Dahbur et al., 2012). Additionally, it is possible for the previously mentioned measures to be defeated by individuals carrying non-metallic explosive devices that cannot be detected by the technology used today (Brown, Sinha, Scchlenker, & Tambe, 2016). According to Price and Forest (2016), the one-size-fits-all system in which every passenger is screened at the same physical point is not only inconvenient but also ineffective because it is inflexible and has too many unnecessary steps that waste time. Price and Forest (2016), advocates for a change in aviation security, want a change that will promote effectiveness and efficiency.

Because of the evolving tactics of terrorists, it is necessary to screen both passengers and their baggage. However, the TSA has not found the most effective and efficient way possible to do this. The agency does not take into account the variations in infrastructure and access points from one airport to another (Dahbur, Isleem, & Ismail, 2012).

It is not known what practices and methods the TSA uses to make decisions for the security system in place today. The current TSA security system has a variety of screening resources, meaning that a broader range of threats can be detected in a more efficient manner (Brown et al., 2016). The current one-size-fits-all system that is commonly used in the aviation industry today may lack the capacity of gathering critical data and utilizing it in a dynamic manner, which would allow different screening mechanisms to be used depending on their effectiveness to that situation (Brown et al., 2016). Further research was conducted to understand why certain protocols and practices were selected and required in the TSA security system.

Additionally, according to Janic (2015), there was much talk about the risk-based assessment measures; assertions have been made that the current security policies should be risk-based because the level of threat and the level of security needed may vary from one airport to the next. Because resources are finite, even for critical matters such as national security, properly allocating these resources among agencies is a critical task (Poole, 2015). Along this line of reasoning, aviation security should concentrate where the threats are the greatest, rather than being spread evenly among U.S airports (Poole, 2015). Conducting threat assessments and risk profiles of airports could help with the efficient allocation of finite government resources. However, the TSA is driven by political imperatives that the public should be made to feel safe no matter what, leading to over deployment of resources in minimal threat areas (Janic, 2015). Therefore, research is needed to determine how and why resources are dedicated to security and

how the TSA makes security related decisions. By better understanding the current security system, successful practices as well as opportunities for improvement can be identified.

Statement of Problem

The problem investigated was how and why the TSA chose to use the current airport security system, as both patrons and colleagues criticized the system for its inefficiencies (Muller & Stewart, 2011; Price & Forest, 2016). While there are several approaches to making decisions when it comes to airport security, there was a need to further look into the methods and reasons that the TSA chose its current security system in order to determine if that system was the most effective and efficient method. The TSA fails to concentrate its resources on where security threats were most acute, instead concentrating on certain demographic groups as potential threats and not tailoring its activities to the threat profile of an individual site of operations (Price & Forest, 2016). The consequence of this problem was the misallocation of finite TSA resources due to an overemphasis on targets and an under-emphasis on the specifics of the site (Poole, 2015). A risk-based system is much more efficient and cost-effective (Wong & Brooks, 2015). Additionally, more research was needed on risk-based screening methods (Wong & Brooks, 2015). Therefore, there was a need to explore the extent to which the TSA utilizes a risk-based method for airport security that would better serve security requirements over a one-size-fits-all method (Poole, 2015; Wong & Brooks, 2015).

In response to the research problem, the results of this study suggest methods that make the TSA equally more effective and more efficient (Price & Forest, 2016). Risk-based models have been employed successfully in the past. These included the TSA PreCheck program and the SURE Concept in the Netherlands (Wong & Brooks, 2015). The TSA's PreCheck program identifies low-risk passengers to expedite the screening process (Beckner, 2015). Beckner (2015)

also stated that the risk-based security method remains the primary strategic imperative for the TSA.

If the problem remains unaddressed, the TSA will continue to operate at less than maximum efficiency. Resources were over-allocated in some locations, leading to unnecessary expense and passenger delay, while other location's resources were under-allocated, potentially allowing threats to slip through the cracks, possibly leading to a terrorist attacks. Such attacks have grave economic and moral consequences for the nation (Bandyopadhyay, Sandler, & Younas, 2014). Hence, there is a need for a risk-based model approach to airport security (Wong & Brooks, 2015).

Purpose of the Study

The purpose of this qualitative single case study was to explore the operations of the TSA in terms of resource allocation and the extent to which the TSA uses or should use a risk-based approach for resource allocation. This was accomplished by gathering secondary data from Government Accounting Office (GAO) reports and congressional hearings regarding TSA operations. The TSA was treated as a single case with two sub-cases: TSA operations from the perspective of the GAO and TSA operations from the perspective of Congressional hearings. Current data and reports were readily available online to the public. The researcher read and analyzed these reports using a qualitative methodology. This involved the use of codes and generation of themes for thematic analysis. All documents were reviewed at least three times to ensure that all pertinent segments of text were coded and that the coding was done accurately. A codebook was created prior to reviewing all documents, which included benefits, known risks, and decision-making. New codes were added to the codebook as needed during the document review. Unfortunately, directly interviewing either senior TSA officials or members of Congress was not possible, as these individuals were not willing or able to discuss matters of national

security. With that said, it was possible to answer the research questions using the secondary data mentioned above, as there was a large quantity of readily accessible data.

Theoretical and Conceptual Framework

The proposed research utilized institutional theory and prospect theory as its framework. The former theory is one of the leading theories used to describe attitudes formulated within an organization and was used to analyze the TSA as an organization and the aviation security system (Scott, 2004). More specifically, institutional theory is concerned with how the players in this given institution, specifically those holding a particular official job or title make official decisions based on their own personal beliefs, biases, or preconceived notions. On the other hand, prospect theory is a behavioral economic theory that examines how individuals decide between probabilities and alternatives (Kahneman &Tversky, 1979). In these cases, the probabilities of various outcomes are more or less known. However, the decisions are based on the potential value of gains and losses, as opposed to the final outcome.

These two theories were appropriate for this study because both theories seek to underline how institutions function overall and how decisions are made that leads to results, such as aviation legislation. These frameworks guided the research problem by specifically investigating how the TSA makes decisions in regard to airport security methods and protocol. In theory, airport security decisions should be made based on components of the theories mentioned; however, it was unknown how TSA made its decisions. It was also unknown if the TSA has reviewed or tested other systems. Thus, the investigation used the institution theory to focus on the institution that enacts the systems in question, as well as the prospect theory to determine the reason why officials have chosen to enact given systems. The purpose and the research questions of this study specifically aim to investigate the various components of the

decision-making process, as well as the advantages and disadvantages of implementing the process, as noted by individuals in the aviation sector.

The concept of institutions was used to mirror the structure of the social environment, in which individuals have to make choices that are based on various factors, such as logic, facts, emotions, and beliefs (Scott, 2004). The prospect theory builds on this decision-making process by describing how choices are made based on an array of factors, particularly on potential gains and losses (Kahneman & Tversky, 1979). Considering institution in a wider sense and how decisions are made, the entire approach to aviation security system is a prime organization to utilize the institutional and prospective approach to explain why aviation security is essential. Furthermore, these theories explain the processes by which people determine the benefits and risks of choosing particular alternatives over others (Kahneman & Tversky, 1979) and adhere to social guidelines. Examples of such guidelines include the rules, routines, schemes, and norms within an organization, all of which are established subsequently as authoritative practices for social behavior (Scott, 2004),

Nature of the Study

The design for this study was a single case qualitative approach, with two sub-cases. Qualitative research was appropriate for capturing the concerns of people's lives and has great promise for making a difference (Merriam, 2014). As such, a single case study method was the most fitting design because it was able to facilitate the investigation of particular events within their actual environment, which cannot be replicated in a controlled environment of a laboratory (Yin, 2014).

The analysis of the data regarding TSA decisions to implement security systems and protocol was done through a thematic analysis method. Colaizzi's (1978) seven-step process was used to analyze data. First, codes were created and defined in a codebook. Then, the data files

were reviewed and text segments were coded with appropriate codes. New codes were added to the codebook during this process as needed. Then, the researcher examined the coded material to generate themes. Themes, or recurring concepts, from the secondary data were identified and recorded as they emerged (Fran, 2013). The researcher used NVivo software to assist in this process. The thematic analysis focused on answering the research questions and is described fully in Chapter 3.

Research Questions

Based on the problem statement for this study, the following research question and sub-questions were developed:

RQ1: How does the TSA decide on efficient airport security systems and how do they adapt their airport security systems?

RQ2: How does the GAO impact the TSA's decision on airport security systems?

RQ3: How do the Congressional hearings impact the TSA's decision on airport security systems?

Significance of the Study

This study intends to contribute to the knowledge base of the best practices of aviation security, particularly with regards to the model by which security is enacted. Security is an issue of great concern and security in the transport sector, specifically in the aviation sub-sector is an issue that should not be overlooked (Wong & Brooks, 2015). The ever-rising and dynamic nature of terrorism and other forms of crime directly threaten the aviation sub-sector. Previous researchers have suggested that air transport is the most vulnerable, and successful terrorist attacks in this mode of transport have been the most financially devastating (Wong & Brooks, 2015). Because of this vulnerability, the types of security systems used in airports were thoroughly scrutinized, since any simple failure could have devastating results (Price & Forest,

2016). Furthermore, not only does aviation security need to be effective, but it also needs to be efficient (Wong & Brooks, 2015). It is currently unknown what factors influence the TSA's decisions to implement or change airport security.

Furthermore, according to Wong and Brooks (2015), there was a need for further research on the merits of risk-based screening, particularly by determining risk potential and mitigation measures much like financial credit risk bureaus. In addition, Brook and Wong (2015) also stated that in the face of future challenges such as increasing the number of passengers, cutbacks from the public sector, and limited resources, it was necessary to find alternatives that may be more effective and financially attractive.

The results of this study will enhance the understanding of the TSA's current one-size-fits-all system and the option of a risk-based system, as well as the legislations and agencies that support these systems. The study's significance does not end with the identification of the discrepancies and weaknesses of the current system but extends to suggestions for wider implementation of the risk-based system.

Definitions of Key Terms

Dynamic. The state of being dynamic is the nature of changing and not being in the same state for a long time (Beckner, 2015).

Enactment. Enactment is the process through which legislation is made and practiced as a law (Price & Forest, 2016).

Jurisdiction. Jurisdiction pertains to independent nations, countries, or kingdoms that have officially recognized governments or dynasties (Edwards, 2013).

Risk assessment. Risk assessment is the state of carrying out an audit on an entity or situation to ascertain the potential risk that it bears (Edwards, 2013).

Screening. Screening is a specialized way of checking for unwanted materials using specialized devices (Edwards, 2013).

Threat. A threat is an object or situation that has the potential to cause harm (Brown et al., 2016).

Summary

The hurried creation and enactment of the ATSA by the American Congress soon after the September 11, 2001, attack led to the establishment of the TSA and the adoption of the current one-size-fits-all system of managing security in all airports (Edwards, 2013). It has proved to be an inadequate system that is inefficient and ineffective in the long run (Muller & Stewart, 2011; Price & Forest, 2016). The purpose of this single case study was to increase the understanding of the factors that impact the TSA's decisions and how those decisions are made to implement airport security systems. This study used a qualitative methodology and a thematic analysis, which involved code creating, coding of text segments, and generating themes within and across codes. Chapter 2 will describe the literature review of applicable research; Chapter 3 will describe the research methods in more depth; Chapter 4 will describe the results; Chapter 5 will discuss the conclusion and limitations and provide suggestions for further research.

Chapter 2: Literature Review

There was considerable debate about the efficacy of TSA's risk-based security measures at airports (Beckner, 2015; Brown et al., 2016; Gillen & Morrison, 2015). While the risk-based security checks were found to be effective, critics pointed to considerable incompetence and misuse that have plagued the TSA (Berghel, 2015; Lowe, 2015; McHendry, 2016; Wong & Brooks, 2015). Consequently, despite the potential and temporary use of the risk-based security approach, there was a need for better implementation and monitoring of this method to ensure efficiency (Greene, Kudrick, & Muse, 2014; Lowe, 2015). In order to assess the true implications of an effective and efficient system, it was necessary to take a closer look at the data. In light of the extant gap in literature pertaining to the efficacy of risk-based security in comparison to the one-size-fits-all method, this study aimed to ascertain how and why the TSA chose the current security system as well as provide a better solution in place of the current system.

The 9/11 terror attacks impacted the security policies not only in America, but globally. While security has always been a major concern for policy makers, the 9/11 attacks brought the issue to the forefront. The sense of imminent threat led several countries across the globe to devote additional funds and resources to preventing terror attacks (Lowe, 2015). Particularly in America, the TSA was formed and commissioned to control counterterrorism operations (Deno, Diaz, Lliguicota, Norman, & González, 2014; Lowe, 2015). The inception of the TSA brought more standardized security methods to airports in terms of screening individuals, carry-on items, and baggage (Lowe, 2015). The TSA implemented rigorous screening for all passengers and baggage check procedures, including X-ray imaging and bomb detection equipment (Lowe, 2015). However, the demanding security procedures of the one-size-fits-all method provoked a

lot of anger from the passengers as these procedures were time-consuming and stressful (Wong & Brooks, 2015). The one-size-fits-all method put severe strains on funds, resources, and employees (Wong & Brooks, 2015). Critics have also found the security measures to fall short of the requirements in spite of the huge monetary investments (Lowe, 2015; Wong & Brooks, 2015). Researchers called attention to the TSA's internal security breaches because of employees' inappropriate behavior and a failure to detect guns and bombs on multiple occasions (Lowe, 2015).

The evolving nature of terror attacks placed additional pressure on the TSA to constantly adapt policies and procedures to prevent and thwart terror plots (Lee & Jacobson, 2012; Price & Forrest, 2016). Amidst all the controversies and growing pressures, the TSA felt the need to reexamine its security measures. The TSA adopted a risk-based process with substantial use of technology to circumvent the problems of the one size fits all method (Clavell, 2015). The risk-based method implemented randomized screening, rigorous questioning of passengers, and tailored risk-based programs (Lowe, 2015; Scurich & John, 2014). The randomized security checks utilized limited resources and helped streamline the existing cumbersome one-size-fits-all method (Beckner, 2015). Programs such as PreCheck, Secure Flight, and Managed Inclusion were implemented to create a quicker and more cost-efficient system (Beckner, 2015). However, in spite of the advantages it offered, the risk-based security check faced criticism from passengers who felt it infringed on their privacy rights and that they experienced racial profiling and biases (Cavusoglu, Kwark, Mai, & Raghunathan, 2013; Deno et al., 2014). Additionally, problems that plagued the TSA under the one-size-fits-all method still threatened its overall functionality. In numerous instances, mismanagement and security failures allowed weapons and bombs to go through the system undetected (Berghel, 2015; Price & Forrst, 2016) and security

breaches occurred from within the organization (Wallace & Loffi, 2014). Overall, the cost-benefit analysis completed by researchers revealed the need for better allocation of funds (Poole, 2015; Shafieezadeh, Cha, & Ellingwood, 2015; Stewart & Mueller, 2013b).

Thus, in light of the above discussion, this chapter took a closer look at the risks, costs, and benefits associated with the operations of both the one-size-fits-all and risk-based security methods and evaluated their shortcomings and efficacies. One of the major purposes of this study was to analyze the decision-making process that operated behind the security policies and procedures. Scott's institutional theory (2004) and Kahneman and Tversky's prospect theory (1979) was utilized to gain insight into the decision-making process to better understand the factors, motives, and reasons that behind decision-making. This chapter captures the important themes and trends associated with the one-size-fits-all and risk-based security methods and provides an overview of the search strategies to ensure that credible and reliable sources were used. It also discusses the theoretical framework and concepts, reviews literature pertaining to costs, benefits, risks, decision-making, advantages and disadvantages of one-size-fits-all and risk-based security methods and concludes with a discussion on the findings of the review.

Search Strategy

Search strategy involved rigorous research through dependable search engines and databases. The primary search engine used was Google Scholar. Academic databases used included ERIC, Elsevier, ScienceDirect, ResearchGate, PsychArticles, ProQuest and EBSCOHOST. Peer reviewed and scholarly sources were selected from the results obtained through searching various words, phrases, and combination of words. The search terms and combinations used included Transportation Security Administration, airport security, Transport Security Administration aviation, TSA, TSA and risk-based security, TSA and one-size-fits-all security, risk-based airport security, risk-based aviation security, security aviation terrorism

threats, advantages of risk-based security aviation, advantages security airport terror attacks, disadvantages security airport terror attacks, benefits risk-based security aviation, costs TSA, costs risk-based security airports, terrorism and TSA, institutional theory Scott, prospect theory, Kanheman, aviation and prospect theory, and aviation and institutional theory. Relevant sources were selected from the list of results. The majority of the sources, approximately 89.33% of the total sources, were published from 2014 onward.

Theoretical Framework

The study utilized institutional theory (Scott's, 2004, 2014) and prospect theory (Kahneman & Tversky, 1979) as the backdrop for analyzing and understanding how institutions function and how decisions were made. Specifically, institutional theory (Scott, 2004) provided a framework for understanding how officials make decisions based on their beliefs and notions. Prospect theory (Kahneman & Tversky, 1979) provided a basis for understanding how risk related decisions were made, and how perceptions about probabilities of gains and losses in outcomes arbitrate those decisions. The following section provides a detailed analysis and the rationale for applying these theories for the current research topic.

Scott's intuitional theory. According to Scott, decision-making and managerial operations of institutions are supported on three pillars: normative, regulative and cultural-cognitive (Scott, 2014). Normative factors refer to norms and habits pertaining to how things are run; regulative factors refer to policies and rules of the workplace, often highlighting legal aspects; and cultural-cognitive factors refer to beliefs and values that shape the rules (Scott, 2014). These three elements work differently for each institution; sometimes one of these elements takes precedence over the others, and at other times, they work in agreement with the others. Scott postulated that the normative, regulative, and cultural-cognitive elements at work in an institution might also change over time. In addition to the tasks or jobs of an institution, its

cultural environment also plays a significant role in how the organization operates. He emphasized how institutions reflect the social structure base on what individuals think and decide based on logic, facts, emotions, and cultural beliefs (Scott, 2014).

Scott (2014) explored the connections between institutional theory and organizational studies, which has created a deep impact on areas such as international business, institutional economics, and political studies focusing on institutions and other related areas. Institutional theory has been used in a wide variety of areas to interpret how personal beliefs and ideas shape decisions. For instance, Pinho (2017; 2016) utilized the theory to understand trends of global entrepreneurship. He saw how the normative, regulative, and cultural-cognitive elements of institutional theory varied across different countries (Pinho, 2017; 2016). Interestingly, the results also revealed that the implications of the regulative and cultural-cognitive factors varied based on a country's focus on production or innovation (Pinho, 2017; 2016). This supports Scott's (2014) assertion that the three elements of institutional theory varied within institutions.

Institutional theory has been utilized to understand change-related decisions of institutions (Palthe, 2014). Thus, Scott's institutional theory can be used as a framework for understanding not only that there are similarities between the common rules and regulations of institutions, but also what the mechanism of change is in institutions (Palthe, 2014). Institutions in general resist change and attempt to maintain the status quo (Palthe, 2014). However, for any change to occur, this status quo or sense of complacency needs to be examined (Palthe, 2014). Palthe (2015) proposed when changes occur in an institution, the regulatory factors pertaining to rules and policies change fast; however, the normative and cultural-cognitive factors related to habits and norms take longer to change.

In the case of aviation security, Scott's institutional theory addressed how culture and beliefs shape the decision-makers' impact on policies, how cultural beliefs play a role in shaping the nature of organizations, how individuals who are part of specific institutions can modify the institutions, and why individuals and organizations adhere to institutions. Thus, the theory was relevant for the current research as it provided a framework that helped explain what factors played a role in the institutional decision-making process as it relates to the security and safety of passengers against terror attacks.

Kahneman and Tversky's prospect theory. Prospect theory (Kahneman & Tversky, 1979), is a behavioral-economic theory that proposes that risk-based decisions are made based on the probabilities of success and failure, or gains and losses. The theory was developed as an alternative model to the most commonly exploited risk related decision-making theory, the utility theory (Kahneman & Tversky, 1979). Prospect theory was developed primarily based on monetary outcome, prospects, and probabilities; however, it can be applied to other areas (Kahneman & Tversky, 1979). Prospect theory builds on this decision-making process by describing how choices are made based on an array of factors, particularly on potential gains and losses (Kahneman & Tversky, 1979). The basic premise of the theory is that the choice process works through two phases, the editing and evaluation phases. In the editing phase, options are organized and formulated to modify the outcomes; this is followed by the evaluation phase, involving assessment of gains and losses and selection of highest value yielding prospects. Kahneman and Tversky (1979) proposed that the certainty effect, the tendency to choose prospects that offer certainty in outcomes over those prospects that are risky or merely probable, often lead people to avert risks. An individual weighs the options and exercises preference over the prospects of a risky situation, assessing them in terms of gains or losses. The individual

prefers or selects the option that offers the maximum utility or benefit. According to the researchers, shape of utility for gains is concave and for losses, it is convex (Kahneman & Tversky, 1979).

Prospect theory has been utilized by researchers and academicians from multiple disciplines to gain better understanding on diverse topics. Abdellaoui, Bleichrodt, and Paraschiv (2007) developed a method to quantify loss aversion at the individual level. Prospect theory helped them discover that loss aversion works both at individual and aggregate levels Abdellaoui et al., 2007). Prospect theory, along with response theory has also been used by researchers to explore test-taking behavior (Budescu & Bo, 2015). When test-takers were aware of the fact that the test scoring involved penalties, it had a negative effect on them, specifically those test-takers who exhibited risk aversion. Penalties in the scoring system also had a negative impact on the test-maker (Budescu & Bo, 2015). Prospect theory and its principles are used in other areas as well, ranging from risk-sensitive reinforcement learning for decision-making under unpredictable conditions, loss aversion affecting human behavior in a soccer match, and loss aversion and risk calculations for market trading (Pasquariello, 2014; Riedl, Heuer, & Strauss, 2015; Shen, Tobia, Sommer, & Obermayer, 2014;2013).

In the case of the aviation industry, Kahneman and Tversky's prospect theory (1979) was both vital and valuable in understanding how decisions were made in situations and events that were perceived as risky. Prospect theory was used to analyze if the choices made by policy-makers and other officials were based on their analysis of the prospects of gains and losses. Finally, it assisted in assessing if risk aversion played a role in the decision-making process and how it affected decisions and procedures.

The two theories together, Scott's institutional theory (2004) and Kahneman and Tversky's (1979) prospect theory provided a basis for understanding the TSA's process and eventual decision to select the current one-size fits all security system. Using the institutional theory provided understanding that the TSA, in addition to other governing bodies associated with aviation security, is an institution that reflects the larger social environment, and the culture within the organization helped bring the rules and regulations together. Several beliefs and ideas played an important role in shaping the rules. Prospect theory helped elucidate the mechanisms and processes that were involved in the chosen policies. Thus, the two theories explained different components of the research questions examined in this study, like benefits, advantages, disadvantages, and efficiency of risk-based and one-size-fits-all security methods. The following literature review section provides a more detailed discussion on the factors that influenced decision-making and how the evolution of the security measures over the years reflects the need for changing strategies with the evolving nature of the terror threats.

Review of Relevant Literature

The purpose of this study was to evaluate in-depth the methods and reasoning behind TSA's decisions regarding the current aviation security system, while examining another potential aviation security system that would better satisfy aviation security requirements in place of the traditional one-size-fits-all method. The following section will recount an extensive literature review to analyze what precipitated the need for a new risk-based security system and the advantages it offers over the current one-size-fits-all method. The literature review was divided into the following broad sections: security prior to formation of the TSA; security under the TSA; new risk-based security under the TSA; one-size-fits-all security vs. risk-based security, including costs and benefits, known risks, decision making processes, and advantages and disadvantages of one-size-fits-all security vs. risk-based security.

Security prior to formation of the TSA. Prior to the 9/11 attacks, the Federal Aviation Administration (FAA) was in control of passenger and cargo security and was responsible for adopting a number of security measures against criminal acts such as hijacking of planes and bringing unauthorized weapons on board (Becker, 2015). Incidents such as the bombing of Pan America Flight 103 resulted in stricter security measures including X-ray imaging of bags and preventing passengers from accessing bags after security checks (Becker, 2015). However, airports and security check experiences for passengers were very different from what they are today. Individuals had easy access to airport perimeters with minimal security checks and even individuals who were not traveling had access to boarding areas (Lowe, 2105). Employees were hired based on meeting nominal requirements, and those who were hired received very little formal training (Lowe, 2015). Overall, it was evident that airport access, airline security, employee and passenger background checks, and employee hiring policies lacked regulation (Becker, 2015; Brown et al., 2016; Lowe, 2015).

Security under the TSA. Things changed in the wake of the 9/11 terror attacks. Aviation security had to adopt very rapidly and strengthen itself against terrorism. Security took precedence over other national interests and concerns. In November 2001, two months after the 9/11 attacks, Congress formed and commissioned the TSA to oversee aviation security and the TSA was given authority over all security measures pertaining to civil aviation to prevent future attacks (Baker, 2015; Lowe, 2015). One of the major changes required criminal background checks of airline and airport employees (Lowe, 2015). The TSA also introduced security measures like the walk-through metal security detectors, checkpoints across the airports, restricting access to gate and boarding areas to ticket holding passengers, additional officers on flights, and some pre-screening programs (Lee & Jacobson, 2011; Lowe, 2015). The role of the

TSA as a counter-terrorism organization was reinforced when the Homeland Security Act transferred the TSA from the Department of Transportation to the Department of Homeland Security (Lowe, 2015).

However, the current aviation security system's one-size-fits-all method became increasingly unpopular among passengers as it required all passengers to go through similar checks and screening processes (Brown, et al., 2016; Lum et al., 2015). These procedures were deemed very demanding in terms of time and patience (Wong & Brooks, 2015). Given the large number of passengers that travelled by air each year, it quickly became difficult to put each and every passenger through the different screening equipment and procedures (Lum et al., 2015). In spite of the comprehensive measures, critics found the security measures incapable of meeting the security requirements (Lowe, 2015; Wong & Brooks, 2015). Overall, the one-size-fits-all method proved to be burdensome in terms of required funds, resources, and employees, and was a major source of passenger dissatisfaction (Wong & Brooks, 2015).

New risk-based security under the TSA. The TSA adopted a risk-based approach to aviation security measures as an enhancement over the one-size-fits-all method that it has utilized since its inception in 2001 (Brown et al., 2016). The risk-based approach was considered to be more efficient in terms of time and utilization of limited resources (Brown et al., 2016). The TSA considered the shift to improve their public image, which was dwindling due to the criticisms that plagued the organization (Beckner, 2015). The risk-based system was able to adapt to the challenges posed by constantly changing threats, which the one-size-fits-all method failed to deliver (Lowe, 2015). It was also designed to utilize minimum limited resources while still delivering high level of security (Beckner, 2015).

One of the major changes implemented by the TSA under risk-based security method was randomization of the checking and screening routines (Scurish & John, 2014; Brown et al., 2016). This allowed the TSA to better utilize its limited resources and employees without compromising the level of security (Scurish & John, 2014). The TSA, under the risk-based security, also implemented segregation of passengers into high-risk, low, or trusted passengers and allowed voluntary enrollment and disclosure options to reduce pressure on equipment, employees, and procedures (Brown et al., 2016; Mills & Reiss, 2014). The PreCheck programs allowed frequent flyer low passengers to preregister and access screening lanes that specifically served them and offered quicker screening and helped reduce the required screening time for those passengers. Depending on the volume of passengers, the TSA allowed low-risk passengers to access the PreCheck lanes under managed inclusion to reduce the load of regular screening (Beckner, 2015).

TSA has benefited from the PreCheck program in terms of providing enhanced security, lesser screening time, and lower costs (Jacobson, Khatibi, & Yu, 2016). PreCheck passengers gain access to quicker security screening lines, although they have to pay the PreCheck fee. As such, several critics argued that PreCheck services should be made free for the registered passengers (Jacobson et al., 2016). Critics also proposed that the no-cost benefits might help TSA to gain more passengers who are ready to enroll for PreCheck services, thus allowing them to sustain high level security while offering expedited screening (Jacobson et al., 2016). However, in spite of the PreCheck program, the TSA's policies and procedures have generated anger and frustration in passengers and critics (Berghel, 2015; Sakano et al, 2016). The TSA's security measures are rife with controversies pertaining to encroachment of privacy rights, racial and ethnic profiling, failing to detect threats, and security breaches by employees. Given the

above scenario, the following sections take an in-depth look into the relative benefits and shortcomings of the risk-based and one-size-fits-all methods and evaluate if risk-based methods ensure higher level of aviation security.

One-size-fits-all security vs. risk-based security.

Costs, benefits, known risk, and decision-making processes. Costs, benefits, risks, and the decision-making process are interrelated and interdependent. While costs are justified in terms of the benefits, there is always limited availability of funds and resources for any organization (Gillen & Morrison, 2015). Decision-making involves assessment of the risk factors, and allocation of limited funds and resources to areas that demand elevated security measures (Gillen & Morrison, 2015; Poole, 2015). Given the complex relationship between these factors, it is important to view them from a holistic perspective and understand how these factors play a role in policies and procedures that are implemented in ensuring airport security (Gillen & Morrison, 2015).

Costs and benefits. Post-9/11 terror attacks, the hasty commissioning of the TSA as a counterterrorism organization led to the implementations of policies and allocation of funds without proper risk assessment (Poole, 2015). This was primarily done to fulfill politically driven motives of pacifying the frightened travelers and assuring them that high levels of security measures were in place (Poole, 2015). Based on the economic principle of opportunity cost, risk assessment is essential to ensure proper allocation of limited resources, as resources assigned to a particular place will not be accessible to another (Poole, 2015). The one-size-fits-all security method attempted to provide nationwide security by implementing screening of all passengers, entrances, and cargo (Scurish & John, 2014). However, as a consequence of the demand for

more resources, equipment, and employees, the one-size-fits-all process was getting harder to sustain given the increase in the number of air travelers each year (Scurish & John, 2014).

In addition to the need for more resources, the one-size-fits-all method is burdensome in terms of required workforce to implement and maintain such extensive security routines, especially because the rigorous security checks have been known to produce exhaustion in and reduce job satisfaction of screeners at airports (Baeriswyl, Krause, & Schwaninger, 2016). The workload and exhaustion of airport screeners affects job performance and can potentially jeopardize safety and security measures (Baeriswyl et al., 2016), which suggested that in spite of policies and funds for supporting all-around security, those measures might fail to yield the desired benefits.

Under those circumstances, supervisor support was found to be a major source of job satisfaction, which could enhance job performance (Baeriswyl, 2016). Thus, in the cost-benefit analysis of the one-size-fits-all method, it appeared that this method entailed extensive usage of equipment, technology, and employees, which was not economically viable (Brown et al., 2016).

Total employee screening is another source of expenditure that the TSA had implemented to reduce inside threats (Price & Forrest, 2016). Reports indicated failure of the TSA workers to detect weapons and firearms from going through the system and of threats originating from within the organization itself (Price & Forrest, 2016). As such, some airports have been utilizing complete screening of employees. The TSA is debating a shift from total screening of employees to inspections of employees, which would incur less expenditure while still maintaining security.

Another side effect of the arduous one-size-fits-all security was the long lines and added wait time for passengers. This not only required more human resources, but also affected passenger decisions pertaining to the selection of flights and customer satisfaction (Elking &

Windle, 2014; Sakano, Obeng, & Fuller, 2016). There was evidence that airport screening time had economic implications as it affects passenger volume and selection of flights (Elking & Windle, 2014). The PreCheck program also benefited the TSA (Brown et al., 2016).

The risk-based security method introduced by TSA supposedly offered a viable option for providing high level of security at reduced costs (Brown et al., 2016). Gillen and Morrison (2015) recognized the dilemma of decision-makers for providing the best security by utilizing limited resources. Gillen and Morrison (2015) examined economic issues pertaining to cost-benefit analysis, use of technology, input and production, flow of information, human elements, performance, and risk-based security methods pertaining to the aviation. Researchers argued that it is hard to assess how much funds came from government and how much money is coming from passengers (Gillen & Morrison, 2015). However, the analysis of the available data revealed that in the near future, passengers may incur more costs in the financing required for aviation security (Gillen & Morrison, 2015).

The two primary benefits of the randomization of security are that it reduces costs and wait time for passengers (Brown et al., 2016; Sakano et al., 2016). The reduced wait time for passengers depends on the availability of resources and personnel and their ability to be effective in screening high-risk passengers and cargo (Beckner, 2015; Brown et al., 2016; Gillen & Morrison, 2015; Lowe, 2015). Further, reduction in wait time increases customer satisfaction and helps serve more passengers (Sakano et al., 2016). The increase in enrollment in the PreCheck program has enabled TSA to reduce the number of screeners, leading to better utilization of staff (Beckner, 2016). This led to a saving of $100 million dollars for the agency in the 2014 fiscal year (Beckner, 2016).

Models estimating the costs, friability, and resilience of air transportation networks when they face critical events like terror attacks or natural disasters have shown that the intensity of the experienced event had an effect on the costs (Janic, 2015). Cost, friability, and resilience are important factors in cost-benefit analysis of airport security (Janic, 2015). Costs refer to additional expenditures incurred due to an event, which could include flight rerouting, delays, and cancellations, which affect passengers as well as the airport and airline personnel. Friability refers to the reduction in the airport network's resilience as a result of removal of certain airport nodes, routes, and links. Resilience refers to the airport network's capability to mitigate the negative impact of disruption due to a critical event. These aspects help airport authorities to maintain resiliency and security measures while continuing to offer service. Janic's (2015) analysis of cost, friability, and resilience of air transportation networks revealed that the experienced events affected the resilience of network. The results also revealed that costs proportionately changed with the intensity of the experienced incident. Although the research was primarily based on a natural disaster and its effects on airport networks, it sheds light on areas of operations that were affected, which in turn may pertain to other disruptive incidents, such as terrorist attacks.

The cost and benefit analysis also revealed how combinations of different security measures could be used to provide optimal security (Shafieezadeh et al., 2015; Stewart & Mueller, 2013b). Given the variety of preventive measures applied to United States aircrafts following the 9/11 attacks, Stewart and Mueller (2013b) looked at the cost-effectiveness of three of the tools: installed physical secondary barriers (IPSB) to restrict access to the hardened cockpit door during door transitions, the Federal Air Marshal Service (FAMS), and the Federal Flight Deck Officer (FFDO) Program. Using a breakeven-model analysis, the authors prescribed

a policy that includes IPSBs, an increased budget for FFDOs, and a reduced budget for FAMS as a viable policy alternative, potentially saving hundreds of millions of dollars per year (Stewart & Mueller, 2013b). Similar to the above study, Shafieezadeh et al. (2015) discussed several security measures and analyzed the results in terms of cost and benefits including TSA's Screening of Passengers by Observation Techniques (SPOT), video surveillance, laser jammer in airplanes to thwart missile attacks, and resilient cargo containers. The results of the study revealed that the blast-resistant cargo containers along with video surveillance of airport premises provided optimal security measures. The findings of the above study revealed the need for flexibility in decision-making to accommodate the best possible economic solutions and adopt security measures to the extent that they are beneficial.

Contrary to the above studies, some researchers have argued whether the risk-based system could be cost-effective. An analysis of airports in the European Union indicated that the policies were not proportional to the airports' sizes or requirements (Amorim da Cunha, Macário & Reis, 2017). It was also found that security measures were appended to existing ones without proper cost-benefit analysis, resulting in increased costs (Amorim da Cunha et al., 2017). The results of the study revealed that although the benefits of risk-based security were apparent, it did not necessarily translate into reduced costs (Amorim da Cunha et al., 2017). Overall, it appears that the one-size-fits-all method is more expensive and requires more resources, screeners, and security officers as all the passengers are required to go through the same security procedures (Gillen & Morrison, 2015; Wong & Brooks, 2015). However, more research was needed to ascertain the cost-effectiveness of the risk-based security procedures.

Known risks. Analysis of how terror attacks have evolved over time reveals the need for counterterrorism efforts to adapt to the nature of the threats (Price & Forrest, 2016; Sandler,

2014). One-size-fits-all security is perceived as ineffective in dealing with the changing nature of terrorism (Beckner, 2015). Researchers have also noted that threats to the one-size-fits-all security system has posed serious challenges and exposed the weaknesses in security measures (Price & Forrest, 2016). The randomized, multi-layered, and data-driven security measures implemented through the risk-based method make it harder for attackers to pass through the system (Gillen & Morrison, 2015). Given the changing nature of terror attacks, it is imperative to identify the emerging trends of terrorism (Lopes, Machado, & Mata, 2016; Sandler, 2014). Some of the emerging trends highlight the differences between domestic and transnational terrorism in terms of causes, economic consequences, and counterterrorism efforts (Sandler, 2014). Knowledge of the types of possible risks might be beneficial for implementing more streamlined security measures.

However, the risk-based system has its own share of criticisms. Some of the major risks pertaining to risk-based security are that the randomization might allow attackers to go through the system undetected and put a regular passenger who possess no threat at risk to be screened excessively (Sakano et al., 2016). In spite of measures such as PreCheck and Secure Flight, which segregates high-risk and low-risk passengers, and lists such as the no-fly-lists and selectee lists that identify potential threats, attackers can find ways to circumvent the security measures or recruit new members not listed as possible threats, who can then pass through the system with minimal checks (de Goede & Sullivan, 2016; Sakano et al., 2016). One way to improve chances of detection is by utilizing technology to expedite the screening methods, which will be discussed later in this chapter (Clavell, 2015).

It is often hard to ascertain passengers' risk levels (Lee & Jacobson, 2012). Researchers have tried to find the best ways for monitoring any alterations in passengers' risk levels,

recognizing that such intelligence could be used to strengthen the aviation security and attune the TSA to the demands of the risks (Lee & Jacobson, 2012). Lee and Jacobson (2012) demonstrated how information can be utilized to detect and quantify threat in passengers as they enter checkpoints, or even through the alarm responses of detection instruments that are part of the security checkpoints. The results indicated the Homeland Security Advisory System could use information to get more accurate real-time data about threats and modify their security measures accordingly to thwart the risks (Lee & Jacobson, 2012).

Another relevant issue is the risk posed by human errors that affects the efficacy of both the one-size-fits all as well as the risk-based security methods. Extensive literature has provided evidence of how an increased workload and a longer shift length affected the performance of baggage screeners and the possibilities of threat detection (Meuter & Lacherez, 2016). The increase in security measures and volume of passengers in recent times has caused screeners to work under a lot of time pressure, which negatively affects their ability to detect threats (Meuter & Lacherez, 2016). Researchers have evaluated threat detection by cabin baggage screeners. X-ray screening at an Australian international airport revealed that screening of higher volumes of bags per minute along with longer shifts negatively affected the rate of accurate threat detection (Meuter & Lacherez, 2016). These findings are supported by Baeriswyl et al. (2016), who found that workload and emotional exhaustion lowered job performance of employees, consequently affecting their capability to detect threats. Skorupski and Uchroński (2015) found that screeners' personal characteristics, subjective natures, and inaccuracies rendered cabin baggage checking inefficient. These studies have revealed that workload and longer shifts jeopardize the chances of threat detection, indicating the need for a more streamlined method of detection in addition to frequent rotation of shifts.

Compared to the one-size-fits-all method, the risk-based security method might be better designed to meet the challenges of the constantly changing nature of terror attacks (Brown et al., 2016). Because of the more regularized and stringent security measures, along with the use of technological innovations and programs such as PreCheck and Secure Flight, the risk-based security screening method provides better security (Brown et al., 2016).

Insider threat is also a primary concern for the TSA (Lowe, 2015). Reports from the Department of Homeland Security (DHS) revealed that several individuals with terrorist ties were recruited by the TSA in spite of the thorough background checks (Lowe, 2015). There are other instances where TSA employees were held responsible for inappropriate behaviors including smuggling, violence, and terrorism (Wallace & Loffi, 2014). As such, in providing recommendations for best practices for security measures, researchers have emphasized the importance for managers and airport authorities to identify potential security threats from within the organizations (Wallace & Loffi, 2014). However, it is equally important to use screening and behavior observation of employees with good judgment, as overemphasis on scrutiny could thwart staff motivation and breed grievance against management (Wallace & Loffi, 2014).

The TSA faced criticism on several occasions for their incapability to prevent weapons and bombs from going through the system undetected (Berghel. 2015). Researchers have found technology, human errors, and faulty procedures to be responsible for the shortcomings (Lowe, 2015). In order to keep a close watch on the human factors involved in the aviation security procedures, the TSA has deployed officers that are entrusted to interact with any human element involved at checkpoint, including officers and passengers (Greene et al., 2014). Thus, the above known sources of risks, namely, human errors, insider threats, and general vulnerabilities in the system warrant changes in the decision-making process.

Decision-making process. Decision-making is critical for every aspect of aviation security, including finance, resource allocation, use of technology, security procedures, hiring employees, and monitoring all security operations. As such, notwithstanding the authority that the TSA yields because of its mandated jurisdiction, it is under constant pressure to assess risk and make correct choices.

Scott's institutional theory (2004; 2014) helped interpret how the regulative aspects of TSA, referring to the rules, regulations, and policies, depend on the normative and cultural-cognitive aspects. The one-size-fits-all method was formulated based on TSA policy-makers' beliefs and values. These values reflect the fears and concerns of the larger social structure of America, and indeed of the world, to prevent another 9/11-like attack. Thus, the security regulations existing during the 9/11 attacks were replaced by new, more stringent rules and regulations. Over time, the one-size-fits-all regulations were falling short of security expectations, especially to meet the challenges of the evolving nature of terror attacks. As such, the TSA introduced new regulations of risk-based security.

As far as the application to the decision-making process is concerned, Kahneman and Tversky's prospect theory (1979) fits in the institutional theory framework. Prospect theory involves editing and evaluating risks and choosing options that have a greater likelihood of success. The new regulations implemented by the TSA reflect the decision-makers' propensity to choose options that offers a degree of certainty. This is particularly relevant to the cost-benefit analysis. Thus, in terms of the policies adopted, it can be argued that the TSA chose to introduce risk-based security in light of utilizing the limited resources and producing maximum gain.

One of the greatest challenges for decision-makers is risk assessment, as a backdrop for security policies and procedures (Poole, 2015). The primary reason for the TSA to shift from the

one-size-fits-all security method to the risk-based security method was the reduced costs of implementation and maintenance (Gillen & Morrison, 2015; Lowe, 2015). Although several researchers regarded this shift as a necessary change, they also called for more vigilance with regard to vulnerabilities in the system (Poole, 2015; Price & Forrest, 2016). For instance, researchers suggested the need for tighter security measures at checkpoints and baggage in the lobby areas, access control for employees, and security coverage of airport perimeters, which otherwise provide opportunities for terrorists to bring bombs into the airport and onto planes (Poole, 2015).

Other researchers have also pointed to the importance of proper risk-analysis to ensure fair allocation of limited resources and finances for improving security measures against terrorism (Chatterjee, Hora, & Rosoff, 2015; Shafieezadeh et al., 2015; Stewart & Mueller, 2013a). Stewart and Mueller (2013a) have provided evidence that security experts tend to be risk-averse when it comes to 9/11 type-incidents, even if it means overspending (Chatterjee et al., 2015; Stewart & Mueller, 2013a). This plays into the hands of terrorists, who instill fear among people and compel them to have second thoughts about taking risks (Stewart & Mueller, 2013a). According to Stewart and Mueller (2013a), the tendency to be risk-averse results in increased spending on security. As such, Stewart and Mueller (2013a) used utility theory and Monte Carlo simulation methods to estimate uncertainties in calculations of net present value, expected utility from the investment and security measures, and probabilities of benefit by implementing specific policy options. They found that even for the most risk-averse security officials, policy changes can cause significant savings at the cost of minimal compromise to security from terrorist acts (Stewart & Mueller, 2013a). The risk-aversion behavior is better understood in the backdrop of prospect theory (Kahneman & Tversky, 1979), which proposes

that people are against taking risks and only choose those options that offer the assurance of success versus those that are only likely to succeed. Decision-makers with high-risk situations want to choose outcomes that offer more certainty. In the TSA's case, the decision-makers chose to over invest because they assessed that it improves their chances of preventing terror.

Similar to Stewart and Mueller (2013a), Chatterjee et al. (2015) also alluded to the over investment by security experts. However, Chatterjee et al. (2015) considered the over investment to be an effect of decisions made by just focusing on one system or layer at a time instead of giving due consideration to the multiple layers of security measures. According to the authors, this over investment results in a loss for the economy and society. They proposed portfolio analysis as a more inclusive alternative, which compares risks, investments, and benefits for all the layers of security, before allocating funds and formulating regulations (Chatterjee et al. (2015).

In another study, Stewart and Mueller (2015) noted that security experts are always grappling with the trade-offs between enhanced preventive measures that result in perceived sense of security and the costs associated with executing such measures. Specifically, the authors explored different dimensions of risk analysis: the cost per saved life, acceptable risk, cost-benefit analysis, and risk communication. In analyzing the risk-based security measures, they concluded that by utilizing the PreCheck component of airport security, significant cost-savings can be achieved, in addition to the considerable efficiencies to the screening process and great benefits to passengers, airports, and airlines (Stewart & Mueller, 2015).

Kahneman and Tversky's (1979) prospect theory provides a framework for understanding how the probabilities of prospects, namely the gains and losses of the one-size-fits-all and risk-based methods, were weighted against each other. While the one-size-fits-all security method

supposedly provided comprehensive security, it failed to yield the desired results in terms of gains, as the monetary costs were larger than the benefits obtained. Thus, decision-makers have always been under pressure, due to the risks associated with replacing a comprehensive security system with a risk-based alternative.

From a decision-making perspective, it is important to ascertain who pays for the aviation security, and this depends largely on identifying who benefits from it (Gillen & Morrison, 2015). Although it might be argued that air travelers should be paying the security services, researchers have pointed out that air travel safety affects everyone, and as such, taxpayers' money could be utilized for enhancing security (Gillen & Morrison, 2015). Like Brown et al. (2016), they found a risk-based security method more efficient (Gillen & Morrison, 2015).

Decision-makers also need to understand how terrorism affects economic aspects and infrastructure of a country (Bandyopadhyay, Sandler, & Younas, 2014). Bandyopadhyay et al. (2014) have indicated that terrorism leads to potential loss of foreign investment. The authors explored, in their theoretical model, the connection between two types of terrorism, domestic and transnational, and foreign direct investment (FDI) (Bandyopadhyay et al., 2014). The results yielded that both types of terrorism negatively affected the flow of FDI (Bandyopadhyay et al., 2014). The researchers reiterated the importance of FDI as a crucial source of savings as well as a mechanism of growth for developing countries (Bandyopadhyay et al., 2014).

One of the dilemmas of decision-making behind public counter-terror spending is that often heavily protected locations are chosen as targets by terrorists (Bausch & Zeitzoff, 2015; Garcia & Winterfeldt, 2016; Goldman & Neubauer-Shani, 2017). According to the authors, citizens choose to visit locations that have high levels of security, and by doing so, they inadvertently become targets for terror attacks (Bausch & Zeitzoff, 2015). Terrorists try to use a

security system's vulnerability to their advantage by selecting a time and location when they can inflict maximum damage (Garcia & Winterfeldt, 2016). Thus, even when their chances of succeeding in a terror attack are limited, they prefer locations with high security with the intention of inflicting heavy casualty and damage (Bausch & Zeitzoff, 2015). On a similar note, Albu (2016) demonstrated how tourist destinations become valued target sites for terrorists. This could reduce visitors and have negative social and economic consequences (Albu, 2016). Goldman and Neubauer-Shani (2017) also found that higher level international tourism could be associated with higher level of terrorist activities in the host country. The results point to a significant relationship between the number of foreign tourists and the number of foreign-terrorist attacks (Goldman & Neubauer-Shani, 2017).

Decision-making pertaining to procedures is closely related to finances and the degree of security needed. Proper analysis of threat and available resources is crucial for implementing the best possible procedures to increase security (Stewart & Mueller, 2013a). Additionally, those security measures need to be efficient in terms of time and convenience for passengers (Gillen & Morrison, 2015). The comprehensive practices under the one-size-fits-all security made it compulsory for all passengers to go through the same number of checks and procedures. In spite of the rigorous checks, the methods failed to maintain high levels of security (Brown et al., 2016). Thus, the TSA adopted the randomized risk-based security method that provided more streamlined procedures, saving time and money (Gillen & Morrison, 2015).

Another important aspect of security procedure is the changing nature of the terror attacks (Sandler, 2014). The one-size-fits all procedures were deemed inefficient to cope with the constantly evolving threats (Wong & Brooks, 2015). Decision-makers opted for the multilayered and randomized risk-based security procedures to enhance security measures (Lowe, 2015).

Several researchers have proposed models to help devise the best strategies for thwarting terror plots (Brown et al., 2016; Cano et al., 2016; Cavusoglu et al., 2013). Brown et al. (2016) proposed a dynamic and randomized game-based threat screening of people and objects at airports that would be more effective in terms of time and cost, and more desirable for screeners as well as passengers. The screening game revolves around the screener and an opponent, in which the screener devices screening strategies involving randomized use of screening resources. The opponent is allowed to view the screening strategy and respond by choosing the appropriate screening categories. The researchers purported that the new risk-based approach is more efficient than the prevalent one-size fits-all screening practices. The risk-based screening, particularly, the Dynamic Aviation Risk Management Solution (DARMS), will help in effective utilization of available resources and managing a larger number of passengers. DARMS focuses on screening passengers based on the risk level assigned to them and the flight they will board (Brown et al., 2016). The researchers considered this to be a more flexible approach which allows screening resources to be used for high-risk passengers and enables the TSA to sustain higher levels of security measures while saving time and resources (Brown et al., 2016).

Similar to the above study, other researchers have investigated the best possible ways to create a security system that would shield against any type of terror attack (Cano et al., 2016; Cavusoglu et al., 2013). Researchers have analyzed the effect of passenger profiling on airport security personnel in circumstances when the profiler is prone to gaming threats by the attacker (Cavusoglu et al., 2013). The researchers utilized Stackelberg's game to simulate the TSA's airport security procedures in which the profiler could be exposed to gaming by attacker. The findings revealed that even though profilers might be exposed to gaming by attackers, it is still important to include profilers for detecting attackers as they reduce costs (Cavusoglu et al.,

2013). The inclusion of adaptive and fuzzy profiling provides a buffer to some extent against gaming by attackers as the profiling methods and strategies are harder to guess. The authors provided recommendations based on their findings for the TSA to follow in order to improve security measures (Cavusoglu et al., 2013). Cano et al. (2013) utilized the adversarial risk analysis (ARA) model to predict an opponent's actions and outcomes for both the defender, which refers to the airport authority, and the adversary, which refers to the terrorist. They believe that the model will help identify the best ways for allocating resources to thwart terror efforts (Cano et al., 2016). Overall, the researchers offered a detailed analysis of how the risk-based security method could be beneficial, as it is harder for attackers to discern and penetrate the randomized routines.

Contrary to the above studies, Scurich and John (2014) found that the traditional one-size-fits-all security measures are able to offer more protection. This study is important from a policy perspective, as passengers are important stakeholders (Scurich & John, 2014). The researchers compared passengers' perceptions about the randomized risk-based security routines with those of the traditional one-size-fits-all method (Scurich & John, 2014). The results of their study indicated that passengers perceived the randomized risk-based routines to be more convenient (Scurich & John, 2014). However, although passengers did not show any frame of reference for either of the methods in terms of effectiveness, they perceived the traditional method to be fairer and more reliable (Scurich & John, 2014). The researchers argued that the randomized risk-based security method has an advantage over the traditional one-size-fits-all method as the method routines were harder to predict, and therefore, difficult for attackers to exploit. Given that terror threats are unpredictable, it is important for the passengers to feel that the security measures will be able to protect them (Scurich & John, 2014). Otherwise, they might

opt for other means of transportations. When it comes to decision-making, policy makers have to find a balance in the tradeoff between what passengers find as convenient and which security method has a greater chance of providing enhanced security (Scurich & John, 2014).

Sandler (2014) identified five aspects of terrorist attacks based on policy perspectives: reasons for terror attacks, economic consequences, and effectiveness of counterterrorism efforts, relationship between terrorism and democracies, and the evolving trends of terrorism. In terms of economic consequences, Sandler (2014) indicated that terrorism has an adverse effect on GDP (Gross Domestic Product). The analysis also indicated that time and space related investigations could also provide valuable insight into the weaknesses in counterterrorism efforts (Sandler, 2014). The researcher suggested that investigations of causes of survival and failure of the various terror groups might also provide relevant information for policy makers and counterterrorism efforts. Policy makers also have to be aware of globalization and increasing demands from commercial airlines (Yadav & Nikraz, 2014). Increasingly, precedence is being given to performance-based regulations rather than the traditional authoritarian regulations established by the national aviation authorities. This shift underscores the importance of policies and regulations needing to change with the evolving times and threat requirements (Yadav & Nikraz, 2014).

In terms of employee related decisions, recruitment and job satisfaction are critical areas for decision-makers. Irrespective of the type of security method used, be it traditional one-size-fits-all or risk-based, employee recruitment constituted a considerable challenge for policy-makers. As discussed earlier, the TSA incorporated intense vetting procedures for more rigorous background checks (Lowe, 2015). However, in spite of the policies and regulations, reports indicated that several individuals with terrorist ties went through the vetting undetected (Lowe,

2015). The drawbacks in the vetting process of employee selection as well as the internal security breaches in the TSA indicates the need for reassessment and monitoring of current policies to ensure proper execution (Wallace & Loffi, 2014). A closely related area to employee performance is the lack of communication and sharing of information within the TSA (Pettersen & Bjørnskau, 2015). In a study conducted in Europe and Norway, it was found that employees believed that security rules and regulations hindered communication and information sharing about safety (Pettersen & Bjørnskau, 2015). Further, the results indicated that the employees considered the rules to be disproportionate to the degree of the threat, making them unjust and unreasonable (Pettersen & Bjørnskau, 2015). The rules and regulations affected job satisfaction, as they were problematic and frustrating for the employees (Pettersen & Bjørnskau, 2015). Thus, it is imperative for policy-makers to reevaluate procedures in order to ascertain their effectiveness.

One of the primary reasons for the inability of TSA employees to improve job performance is the lack of training (de Gramatica, Massacci, Shim, Turhan, & Williams, 2017; Kirschenbaum & Rapaport, 2017). Researchers have underlined the importance of providing appropriate training to airport security officials, as it has direct consequences for maintaining and improving security measures (de Gramatica et al., 2017). This has important policy implications for both the one-size-fits-all and risk-based security methods, as the training of officials is an expensive process and often the amount and type of training required is not clear from the data on human errors and performance levels (de Gramatica et al., 2017). In a study conducted by de Gramatica et al. (2017) in a high-level risk airport in the Eskisehir area of Turkey the researchers found that training enhanced security staff members' motivation to put optimal effort in maintaining security. Further, results of the study indicated that specialized or technical training

in comparison to general training was more important for job performance as well as job retention purposes (de Gramatica et al., 2017). Kirschenbaum and Rapaport (2017) underlined how employee training affects compliance with job rules. The results of their study, conducted in airports across Europe, found that there was a gap in the practical application of the training in the real world (Kirschenbaum & Rapaport, 2017). They encouraged decision-makers to take into consideration the experience level of the trainees and the expectations of the job (Kirschenbaum & Rapaport, 2017).

Researchers have suggested that shortcomings, near misses, and accidents provide opportunities for learning (Dillon, Tinsley & Burns, 2014; Madsen, Dillon, & Tinsley, 2016; Paté-Cornell & Cox, 2014). Paté-Cornell and Cox (2014) identified three critical aspects of risk analysis: risk assessment, risk management, and risk communication. The researchers highlighted that the process of risk analysis could be enriched if it incorporated learning from near misses (Paté-Cornell & Cox, 2014). They alluded to the fact that often failure leads to criticism and blame (Paté-Cornell & Cox, 2014). However, productive appraisal of the same failure or near-miss situation could inform decision-makers (Paté-Cornell & Cox, 2014). Madsen et al. (2016) also noted how decision-makers could benefit by considering near misses to formulate safety measures. Further, Dillon et al. (2014) suggested that the near miss events act as reference points for the public to assess the event in terms of other attacks. They also encouraged policy makers to understand the nature and scope of attacks before formulating security regulations (Dillon et al., 2014).

The above discussions brought some of the key issues related to aviation security decision-making and the factors that influence decision-making. Scott's institutional theory (204; 2014) and Kahneman, and Tversky's (1979) prospect theory have provided a backdrop for understanding how these key factors along with the cultural milieu and personal characteristics of the policy-makers shape decisions. In the final analysis, it will be beneficial to weigh the advantages and disadvantages of the traditional and the new risk-based security methods in providing enhanced protection.

Advantages and disadvantages. The introduction of TSA's risk-based security points to the inherent deficiencies in the one-size-fits-all method in providing aviation security (Beckner, 2015). However, one-size-fits-all method is not without its advantages. The critical question is the degree to which these advantages are effective in implementing smooth security operations and whether or not these advantages are efficient and cost effective.

Advantages of one-size-fits-all security. The greatest advantage of this method is that it provided comprehensive security coverage after the 9/11 attacks. This method incorporated several security measures and devices, like background checks, X-ray imaging, and screening that were valuable in ensuring safety and security for passengers (Lowe, 2015). Passengers felt that the one-size-fits-all security method is more reliable in providing protection (Scurich & John, 2014). Studies on passengers' perceptions about the two types of security have revealed that passengers are willing to sacrifice convenience in exchange for more security (Sakano et al., 2016; Scurich & John, 2014). Additionally, the one-size-fits-all security system is considered to be more equitable than risk-based security (Scurich & John, 2014). The fact that one-size-fits-all security system requires all passengers to go through the same security measures reduces chances of profiling. However, this notion is contested by researchers as they believe the notion

of saftey depends on passengers' perceptions of fairness rather than actual evaluation of the security practices (Scurich & John, 2014).

Disadvantages of one-size-fits-all security. Some of the major concerns relating to the one-size-fits-all method are that it is cumbersome and expensive (Wong & Brooks, 2015). The method, which requires every passenger to go through the same and equal number of screening devices, is less effective in handling the growing number of passengers in limited spaces (Wong & Brooks, 2015). The cumbersome procedures were time consuming and required a large number of security personnel (Lowe, 2015). As a result, the procedures became a source of passenger dissatisfaction (Sakano et al., 2016). Researchers have also argued that the wait time for the security checks could act as deterrents for passengers' flight selection (Sakano et al., 2016). In spite of the large amount of spending to maintain comprehensive security, the one-size-fits-all method has failed to provide the required level of security (Gillen & Morrison, (2015). Some of the major criticisms of the one-size-fits-all method's inability to provide desired security include an inability to cope with constantly evolving nature of terror attacks (Brown et al., 2016),the high probability of terrorists manipulating the predictable security routines to their advantage, and the probabilities of internal threats (Wallace & Loffi, 2014). The one-size-fits all method fell short in keeping up with the novel ways that terrorists planned their attacks (Beckner, 2015). Researchers have expressed concerns over the probabilities of attackers to circumvent the known procedures to launch a successful attack (Scurich & John, 2014). They have proposed game-based security models to establish the efficacy of a risk-based system in reducing chances of attacks (Brown et al., 2016). As mentioned earlier, TSA employees have been found responsible for offenses, which resulted in security threats (Wallace et al., 2014). The arduous security checks could also affect job performance of the employees (Baeriswyl et al.,

2016). Researchers have found that higher volumes of baggage checking within a given amount of time negatively affected performance, which could make the security susceptible to failure (Baeriswyl et al., 2016). Thus, given the broader analysis of the advantages and disadvantages of the one-size-fits-all method, it appears that the system needed to incorporate strategic changes to address security concerns while being cost effective and time efficient. Just like decision-making under risk-based approach, the one-size-fits-all security needed to strike a balance between the level of security and the amount of economic investment.

Advantages of risk-based security method. One of the greatest advantages of a risk-based system is the randomization of security checks (Scurich & John, 2014). Randomization has offered multiple advantages over the traditional method, including better utilization of resources at much reduced costs (Scurich & John, 2014), improved security making the system less predictable and more difficult to breach, (Scurich & John, 2014), and streamlined security measures, which are perceived by passengers as more convenient (Lowe, 2015; Sakano et al., 2016).

Other researchers focused on the efficiency of risk-based security in optimizing resources (Brown et al., 2015; Wong & Brooks, 2015). The researchers argued that segregating high-risk passengers from low-risk passengers and devising screening strategies and methods accordingly has led to optimal utilization of resources (Wong & Brooks, 2015). However, researchers have pointed out that the new risk-based approach will necessitate more flexibility from airport authorities, airliners, and passengers (Wong & Brooks, 2015). There will also be a need for more transparency and open conversations between state and federal agencies (Wong & Brooks, 2015). Brown et al. (2016) purported that the risk-based screening, particularly the Dynamic Aviation Risk Management Solution (DARMS), will effectively utilize available resources and

help manage a larger number of passengers. The risk-based approach enables the TSA to sustain higher levels of security measures while saving time and resources.

The TSA PreCheck program has made a major contribution to the efficiency of the screening process (Beckner, 2015; Jacobson et al., 2016). TSA PreCheck offers expedited screening while saving costs and providing enhanced security (Jacobson et al., 2016). The PreCheck program has reduced costs by streamlining the screening process as well as the required workforce (Jacobson et al., 2016). The program has achieved its goals through direct enrollment and managed inclusion of passengers into PreCheck lanes (Beckner, 2015). The TSA is currently exploring ways to increase enrollments by incorporating the private sector to sustain PreCheck's growth and efficiency in terms of operations and security (Beckner, 2015).

Another advantage of risk-based security is employing a specialized workforce team to oversee the human elements of the TSA (Greene et al., 2014). These specialized officials, also referred to as engineering psychologists, add value to the risk-based security method, as they are responsible for overseeing a broad range of tasks. These officials are entrusted with any human element involved at checkpoints. This includes officers as well as passengers. The TSA attempts to incorporate specialists from multiple disciplines to improve human experiences and increase efficiency. The incorporation of these officials reveals the TSA's efforts to closely monitor the human elements that factor into the efficiency of the security system.

One of the greatest advantages of using technology under the risk-based security method is that minimizes risks through predictive and preventive measures (Clavell, 2015; Egbert & Paul, 2015). The use of data-driven technology has improved precision, speed, and accuracy (Clavell, 2015). Clavell (2015) indicated that the use of technologies such as Big Data have made more resources readily available and enhanced performance of security operations. He

explored how privatization of security operations has augmented the incorporation of technology and supposedly reduced costs. Other researchers have indicated how lie detectors are being used for preventive measures as part of counterterrorism efforts (Egbert & Paul, 2015). However, Clavell (2015) stated that the use of technology also demands flexibility and major changes in infrastructure, policies, and functions.

Contrary to Clavell (2015), other researchers highlighted the downsides to an overwhelming dependence on technology (Fox, 2016; Schmidt, 2016; Vorobeychik & Letchford, 2015). While Vorobeychik and Letchford (2015) reiterated how technology helps in information gathering, sharing, and decision-making, they also pointed out how the interconnected technology systems are vulnerable to cyberattacks, in which an attack on one system can make another vulnerable, which can then spread to other systems across the globe (Vorobeychik & Letchford, 2015). The researchers emphasized the need for making the system infrastructure resilient in order to prevent attacks from spreading from one destination to another (Schmidt, 2016; Vorobeychik & Letchford, 2015). Fox (2016) also warned about cyberattacks that could target aircrafts and underscored the importance of preparing for such threats.

The multi-layered security of the risk-based method has bolstered the procedures to be more effective (Chaterjee et al., 2015). The basic concept behind the multi-layer strategy is that under randomized security, if an attacker gets past one layer undetected, they will get caught in another one (Jackson & LaTourrette, 2015). Jackson and LaTourrette (2015) also reiterated the rationale behind layered security in which consecutive strata of hurdles are implemented, with the idea that the weaknesses of one are compensated in the other layers. The researchers emphasized that while those layers of security can help strengthen the system, they can also destabilize or undermine each other (Jackson & LaTourrette, 2015).

Researchers have noted that terror activities targeting the aviation industry have declined in recent years (Barnett, 2105). Barnett (2015) analyzed data from successful terrorist attacks across the world between the years 1982–2011 to assess whether attacks have increased. His analysis revealed that terrorist attacks on aviation were carried out predominantly in the earlier years, while rails attacks have become more prevalent in later years; overall, attacks have gone down in numbers in recent years (Barnett, 2105). It is, however, arguable whether the trend reflects improved security or a shift in terror tactics. Barnett (2015) warned against being complacent with this trend. He encouraged constant vigilance and efforts to strengthen security measures. According to Barnett (2015), successful attacks have long lasting effects on society and might be viewed by terrorists as triumphs encouraging them to engage in further violence.

Disadvantages of risk-based security method. One of the greatest controversies surrounding risk-based security pertains to infringement of privacy rights (Cole, 2015; Deno et al., 2014; Lum et al., 2015; Valkenburg & van der Ploeg, 2015). The relationship between security and human rights is complex (Lum et al., 2015). Risk-based security practices incorporating the use of X-ray imaging, scanners, active millimeter wave scanners, metal detectors, and pat down methods have invasive consequences for passengers (Valkenburg & van der Ploeg, 2015).

Interestingly, Valkenburg and van der Ploeg (2015) indicated that often security technologies, which are introduced to circumvent inequalities in treatment and protect privacy, might produce the opposite effects. Researchers analyzed and noted that over the years, security has become more and more invasive (Valkenburg & van der Ploeg, 2015). While security initially focused on visibility of baggage and cargo, now it demands pictures of the human body (Valkenburg & van der Ploeg, 2015). Body scanners and active millimeter wave scanners are

examples of equipment that have generated grievances from passengers, particularly women (Deno et al., 2014; Valkenburg & van der Ploeg, 2015).

This is also supported in the research by other authors who studied the use of full body scanners (Prezelj, 2015). With today's increased terrorist threats, it is important to use devices such as body scanners and X-ray machines that can detect concealed weapons and risky items (Prezelj, 2015). However, those devices are perceived as violating privacy and human rights. As such, it is important to find a balance between providing security measures while maintaining human dignity and rights (Prezelj, 2015). Prezelj (2015) also noted that it is important to recognize and acknowledge that human security, by its very definition, also upholds the rights of individuals. This provides a novel perspective in understanding the true relationship between security and human rights and revealed how devices such as body scanners can be utilized with discretion to respect human rights while ensuring security.

Modern democracies have significantly encroached upon human right in return for providing security (Cole, 2015). Researchers have debated the trade-off between human rights and protection from threat (Bonfanti, 2014; Cole, 2015; Deno et al., 2014). Deno et al. (2014), in analyzing the security techniques utilized by the TSA, noted that security procedures could be potential threats to privacy. They alluded to manual search and pat down procedures, which passengers find to be invasive (Deno et al., 2014). Additionally, the use of data-driven technology has not only given the screeners access to private information, but the TSA is also responsible for managing the huge amount of passenger data (Deno et al., 2014). Bonfanti (2014) investigated how the use of sniffer devices to detect traces of explosives in certain airports in Europe raised concerns about privacy rights. Passengers have also complained about being

subjected to secondary checks and pat down searches because of their ethnic or racial origin (Deno et al., 2014).

Another closely related issue is racial and ethnic profiling (Ergün et al., 2017; Lum et val., 2015; Welch, 2016). Risk-based screening has been perceived as being vulnerable to abuse, because screeners can profile and harass passengers depending on their gender, race, or ethnic background (Cole, 2015; Welch, 2016). Welch (2016) alluded to the connection made between the 9/11 terrorist attacks and people from Arab or Muslim countries in public perception. The researcher suggested that the 9/11 incidents and preventive measures adopted for averting such attacks have led to more profiling of minorities on the pretext of preventive measures (Welch, 2016). As such, Welch (2016) concluded that people of Middle Eastern or Muslim origin were stereotyped and felt the effects of minority threat.

Comparable studies focusing on perceptions of differential treatment of passengers based on age, gender, and racial origin by airport security officials have found that there was considerable discrepancy in treatment based on racial groups (Ergün et al., 2017; Lum et al., 2015). Lum et al. (2015) indicated that nonwhite passengers were put through more rigorous screening than their white counterparts. The nonwhite passengers also had more items seized without any clarifications (Lum et al., 2015). The authors emphasized that it is important for TSA officials to demonstrate more professionalism and treat every passenger with respect and provide proper reasons for their actions (Lum et al., 2015). Ergün et al. (2017) conducted a study at one of Turkey's airports and discovered that security procedures are sources of heightened tension and anxiety for passengers, especially for those of Muslim and African origins than for passengers of European origins. The authors recommended proper measures to reduce passenger stress and anxiety related to security procedures, such as the use of biometrics. In addition, the

authors underscored the importance of promoting the cognitive growth of the security personnel through training and other resources (Ergün et al., 2017).

One issue that inevitably comes up with the use of advancements in technology and big databases is the trade-off between availability of data and the sanctity of personal and sensitive information (Leese, 2014). Racial profiling and discrimination are unwelcome side effects of the use of data-driven technology in the fight against terrorism (Leese, 2014). However, given the advancement of technology and the consequent availability of complex databases, the researchers explored constructive ways of utilizing such tools to fight terrorism more effectively (Leese, 2014). Against this backdrop, Leese proposed knowledge-generating algorithms on anti-discriminatory safeguards. They found that it is hard to preserve the tenets of fundamental rights and anti-discrimination (Leese, 2014).

Other researchers have pointed to the security breaches and procedural misuse and misconduct by security personnel (Berghel, 2015; Rudner, 2015; Wigginton, Jensen, Graves, & Vinson, 2014). Berghel (2015) noted that under the risk-based security, weapons, bombs, and potential threat items have passed through the system undetected. Rudner (2015) indicated that the layered structure of risk-based security was designed to create a formidable security system, where if a threat passes through one layer undetected, it will be detected in the others. In spite of that, terrorists have been able to circumvent the security measures due to negligence of the employees or deficiencies in the system itself (Rudner, 2015). Wigginton et al. (2014) noted that behavioral profiling has been exploited by security personnel who are meant to use it for monitoring passenger behavior.

The corruption within the TSA is another disadvantage which has become apparent through several incidents related to the screening method (McHendry, 2016). McHendry (2016)

drew attention to some of the failures in the TSA's screening methods. McHendry questioned the notion that current surveillance methods facilitate security operations. He provided several valuable viewpoints in assessing the current security measures at airports and pointed to numerous shortcomings in the security procedures that need to be addressed (McHendry, 2016).

Leese (2016) analyzed the effects of outsourcing security services to private sector firms on the quality and value of the security services provided. The results of the analysis revealed that marketized security services create more flexibility for government agencies and reduce costs (Leese, 2016). However, the contracting of security operations from the private sector has several disadvantages (Leese, 2016). One of the main downsides is that, along with the operations, there is transference in accountability and authority. The author suggested that marketized security services reduced the quality and value of the services provided (Leese, 2016).

Another negative aspect of the TSA's risk-based security is that employees face task segregation in terms of gender (Chan & Anteby, 2016). Chan and Anteby (2016) noted that duty and task segregation lead to inequalities and has had negative repercussions on the quality of work. Researchers found that there is a disproportionate allocation of women to pat-down jobs, which involves manual screening of passengers for detection of prohibited items (Chan & Anteby, 2016). The inequitable allocation of female workers to one particular kind of task led to poor performance. This also led to the female employees being exposed to higher levels of physical stress, exhaustion, and severe emotional strain with relatively few resources for coping. In addition, female workers were at the mercy of managerial approvals for taking leave and had limited scope for improving their skills. These limitations appeared to hamper their prospects for promotions and better earnings, resulting in lower job satisfaction and higher turnover rates.

Summary

The primary objective of the current research was to determine how and why the TSA chose the current one-size fits all approach to airport security. The review of literature has demonstrated how the 9/11 terror attacks have transformed the government efforts to subvert and thwart threats. The formation of the TSA and the implementation of the one-size-fits-all security method, and later the temporary use of the risk-based security method, bear testimony to the organization's efforts at meeting the evolving nature of terror threats.

The analysis of the costs, benefits, and risks have revealed that the one-size-fits-all method is expensive and falls short of providing the required level of security in spite of its comprehensiveness. The TSA introduced the newer risk-based approach, as it has the potential to offer higher level of security at reduced costs (Wong et al., 2015). However, its randomized security methods were scrutinized and criticized for infringing on privacy rights, racial profiling, and security breaches (Berghel, 2015).

The literature review revealed some important trends pertaining to the efficiency of risk-based security method. It appears that in order for the new system to yield the desired results, airport authorities, airliners, and passengers have to be more flexible. At the same time, there is a need for transparency and open conversation between states and federal agencies (Wong Brooks, 2015). Further, the review of literature also illustrated that it is not enough to draw policies and implement procedures. The execution of those procedures is prone to human errors, unseen vulnerabilities, technical glitches, misuse, and new and unprecedented risks. In addition, there might also be errors in the design of the policies. As such, it is of utmost importance to follow up on the procedures, monitor employees, assess the effects on passengers, and analyze the efficacy of risk-based security method to achieve desired outcomes.

Chapter 3: Research Method

The problem that was investigated is how and why the TSA chose to use the current airport security system, as it has been criticized for being inefficient by travelers and colleagues (Muller & Stewart, 2011). Although a multitude of methods aid in creating airport security policies and practices, there was a need for in-depth research into how and why TSA chose its current security method, to ensure that it is indeed the most effective and efficient method. The TSA tends to focus on certain demographic groups as potential threats rather than the threat profile of an individual site of operations (Price & Forest, 2016). The purpose of this qualitative single case study was to explore the operations of the TSA in terms of resource allocation and the extent to which it uses or should use a risk-based approach allocation. To address the problem and to realize the intended purpose of the study, the researcher used a qualitative methodology with a single case study using secondary data. The TSA was treated as a single case with two sub-cases: TSA operations from the prospective of the Government Accounting Office (GAO) and the TSA operations from the perspective of Congressional hearings.

This chapter discusses the details of the procedures and methods that were implemented to fulfill the purpose of the study and find out the answers to the research questions. This chapter also discusses the research design, which was a qualitative single case study, and the data collection, sample and sampling procedures, materials and instruments, study procedures, as well as the data analysis. Finally, the methodological assumptions, limitations, and delimitations are examined. A chapter summary will be provided at the end.

Research Method and Design

The research design for this dissertation was a qualitative case study. Yin (2013) claimed that a researcher is aware that using a case study approach or design is appropriate if there is a need to investigate a phenomenon using the perceptions of individuals in a group with a distinct

set of characteristics pertaining to the phenomenon in question. A qualitative methodology was appropriate for this study because there was a need for in-depth exploration of a phenomenon (Katz, 2015). Understanding and exploring a phenomenon that requires rich data sets and worded answers is suitable for a qualitative methodology (Katz, 2015). Through this method, the researcher explored the perceptions of experts in the field of aviation and airport security to gain a deeper understanding of the phenomenon of why and how the TSA came to decide to use the current airport security system. Based on the problem statement for this study, the research questions are as follows:

RQ1: How does the TSA decide on efficient airport security systems and how do they adapt their airport security systems?

RQ2: How does the GAO impact the TSA's decision on airport security systems?

RQ3: How do the Congressional Hearings impact the TSA's decision on airport security?

The researcher considered other research designs for this study, but a single case study was found to be the most suitable to address the purpose of this study. The researcher found that phenomenology was not suitable for this study because the intended focus is not on the importance of the lived experiences of the phenomenon but the perceptions of the individuals about the phenomenon (Moustakas, 1994). Grounded theory was also inappropriate for this study because the researcher does not intend to develop a theory from the data collected from aviation security experts (Glaser, 1992). Narrative inquiry was also not appropriate for the study because there was no need to collect and analyze data based on the order of occurrence or arrange them in chronological order to fulfill the purpose of the study (Connelly & Clandinin, 1990). Therefore, the case study approach was chosen as the research method for this dissertation.

Population and Sample

According to Creswell (2009) most research is initiated in order to examine what is already known and what remains to be discovered about a specific topic. Unfortunately, it was impossible to directly interview both senior TSA officials and members of Congress. Aside from having access to secure interviews with senior personnel in the TSA and Congress members, said members are not willing or able to discuss matters of national security. With that said, it was possible to answer the research questions using secondary data. Therefore, this research study used an extensive comprehensive literature review of secondary data to investigate past and present work of experts specializing in the field of airport security. According to Heaton (2008), the use of secondary data for research has increased exponentially.

The use of secondary data in research was first introduced by Glaser (1963), who simply stated that there is potential in reusing data that was collected for a different purpose (as cited in Andrews, Higgins, Andrews & Lalor, 2012). For this study the researcher gathered secondary data from various organization and resources, such as the Government Accounting Office (GAO) website. The GAO website has documentation on research audits, policies, and much more. Another source for secondary data for this research was the Government Publication Office (GPO). The GPO is responsible for publishing and making available to the public documentation pertaining to all three branches of the United States Government. The researcher also used other sources such as EBSCOHOST, Google Scholar, and ResearchGate.

In order to ensure that the reports and documents were pertinent to the purpose of the current study, they had to satisfy a set of criteria for eligibility. The inclusion criteria for the documents were the following areas of inquiry: cost, benefits, known risks, and decision-making.

The creation of a codebook prior to evaluating data assisted the researcher with identifying data that met the aforementioned criteria for eligible data. This allowed the researcher to identify patterns and themes within the data.

Material and Instrumentation

The materials to conduct this research were collected by gathering secondary data. Secondary data, such as reports, documents, and congressional hearing interviews, were collected from the GAO, TSA, and congressional hearings. The previously mentioned data has original, vital, first time accounts of the initial decisions made and the outcome that assisted with answering the proposed research questions.

With that being said, there was no better place to start looking for answers to the research questions than with the creation of the TSA. The TSA was tasked to create the airport security system that is currently in place. However, there were no clearly documented reasons behind why and how the TSA decided upon the current system (Muller & Stewart, 2011). In order to get a clear picture and understanding of the TSA's current system, there was a need to review past and present data, which was done by using the appropriate instrument, secondary data.

The secondary data was collected from reputable and reliable sources that spearheaded the creation of the current airport security system. The latter was conducted by exhausting online sources such as the GAO, TSA, and GPO along with reports, documents, and congressional hearings that met the outlined criteria pertaining to cost, benefits, known risks, and decision-making. According to Pierce (2007), indicators of reliability are if the secondary data was obtained from someone who was a participant or an observer of the phenomena. Pierce (2007) also stated that a critical indicator of reliability when utilizing secondary data is the relation of the timeframe or proximity of the data collection to the phenomena being investigated.

Operational Definitions and Variables

Data was collected using secondary data. Secondary data was collected from websites, databases, and literature. The data included congressional hearings and interviews, reports and documents, and literature. A codebook was formulated to ensure that the advantages and disadvantages of the variables, which were cost, benefits, known risks, and decision-making, were easily identified. A second codebook was created for coding in NVivo. The codebook was used to identify if data covered any of the following categories: cost of airport security prior to the TSA, changes to cost after the creation of the TSA, the benefits to the current airport security system method, benefits of another airport security method, the decision-making process involved in the formulation of the TSA, the decision making process of changing specific aspects of the TSA, and the known risks of the current airport security system.

All data was imported into NVivo. The data was reviewed twice in NVivio, and codes from the second codebook were applied to segments of text during this process. The coding consisted of open coding, axis coding, and selective coding. Descriptive analysis of the codes was conducted. This involved obtaining the frequency of the codes and common occurrences of the codes, meaning when segments of text contained the same two codes multiple times. Themes were generated from examining text segments that shared the same code, as well as cross codes themes regarding the data, also known as the fundamental structure step.

Study Procedures

The Colaizzi seven-step method was used for this study. Secondary data was collected using congressional hearings and interviews, reports, and documents. The first step in data collection was the preparation of materials. A codebook was created prior to collecting data. The codebook assisted the researcher in distinguishing which data would be useful for this study. The latter was accomplished through use of the eligibility criteria of data and by only gathering data

that pertains to the cost, benefits, known risk, and decision-making in the current airport security system. All significant statements were numbered and placed on a list. In the next phase, the researcher created general meanings of each statement on the list. There were seven categories of general meaning that significant statements fell into. The seven categories are as follows: cost of airport security prior to the creation of the TSA, changes to cost after the creation of the TSA, the benefits to the current airport security system method, benefits of another airport security system method, the decision making process involved in the formulation of the TSA, the decision-making process of changing specific aspects of the TSA, and the known risks of the current airport security system. According to Colaizzi (1978), the categories will allow the researcher to establish and formulate theme clusters. The researcher then developed and grouped the theme clusters into categories based on specific criteria such as cost, benefits, known risks, and decision-making.

Using the findings of the theme clusters allowed the researcher to move on the next phase described by Colaizzi (1978) as the fundamental structure step. The fundamental structure step is the phase in which the researcher conducts an in-depth analysis of the theme cluster data to find the essence of the phenomena. In last stage of the study, using Colaizzi's procedure, the researcher revisited the data documentation, reports, and hearings to ensure the essence of the phenomena was articulated and described fully. At this point alterations were entered or corrected and included.

Data Collection and Analysis

Data was collected from two main sources: the GAO website and the United States Government Publishing Office. Each of these databases offers extensive documents pertaining to the TSA and congressional hearings. However, the search for adequate documents also included Google Scholar, ResearchGate, and EBSCOHOST. The initial collection phase involved

gathering as many reports and documents that are pertinent to the study based on the eligibility criteria of costs, benefits, known risks, and decision-making. This involved an extensive search through the databases until all related reports and documents were located. Each report was then examined for inclusion. Next, the data analysis phase began.

The researcher conducted a thematic approach to analyze the data for this single case study. All the data was loaded into the NVivo software prior to the analysis. The NVivo software was used to help the researcher process a large amount of textual data from the documents and reports gathered in the data collection phase. Specifically, the researcher used the NVivo software to code the data and group the codes into themes that were relevant to the research topic and research questions.

When performing the thematic method of analysis, the researcher, as the analyst, underwent three major phases of coding: open coding, axial coding, and selective coding (Fram, 2013; Olson, McAllister, Grinnell, Walters, & Appunn, 2016). Open coding is a process of identifying relevant terms to reduce data into manageable segments (Olson et al., 2016). In the open coding phase, the researcher read and re-read the data collected. While performing the readings, the researcher categorized the reports and documents text into small segments by determining only those that were relevant to the research questions of the study. From these segments, the researcher developed the coding system that was needed for the analysis of the entire data set (Fram, 2013). After reviewing the data and developing the coding system, the list of open codes was summarized.

Axial coding is the process of connecting the codes into meaningful groups (Fram, 2013). The researcher performed axial coding by analyzing the list of codes that was developed in the open coding process. The researcher identified possible groupings of the codes and identified

relationships between the groups of data. From this process, the researcher formed the themes that were relevant to answer the research questions of the study (Kolb, 2012). The researcher then repeated the open and axial coding phases for the other data sets until all cases were coded and thematized. The researcher then proceeded with the selective coding phase.

The selective coding phase involved the process of reviewing all the themes from the different secondary data and determining the ones that had a direct relationship to the research questions (Fram, 2013; Olson et al., 2016). For this study, the researcher determined the common emergent themes from the major areas of inquiry: cost, benefits, known risks, and decision-making; major themes were then identified. The themes that aligned with the research questions but were directly related to the inquiry of costs, benefits, known risks, and decision-making were identified as sub-themes. The researcher then developed a concise report of the final results (Fram, 2013; Olson et al., 2016).

Assumptions

The researcher made several assumptions in this study to ensure that the implementation of the methodology was successful. The first methodology-based assumption was that the documents and reports were truthful and extensive in the information reported.

The researcher had to assume the truth in the data because of the lack of control over the reports and documents since they were compiled by other people. The assumption had to be made for the researcher to carry out the study.

Another assumption related to methodology is that the researcher uncovered emergent themes from the data. The researcher was able to offer a new perspective that will add to existing the knowledge base. By making this assumption, the researcher was not influenced by the perceived pressure of making data consistent across other data, reports, and documents while collecting data.

The researcher also assumed that the sample of selected documents and reports was sufficient to reach data saturation. According to Yin (2013), a sample of 6 to 10 would be enough to reach data saturation provided the documents have the characteristics that are needed for the study. This assumption was made in order to prevent the researcher from collecting an endless number of documents, which is not feasible because of the constraints of limited time and resources.

Limitations

The researcher identified a few limitations for this study associated with the secondary data. The first limitation was that the secondary data was collected and presented by an outside source; therefore, the data could be inaccurate or manipulated. The researcher had to assume that those individuals presenting the data were reputable and honest. The second limitation is that secondary data may be incomplete or represent a limited or partial perspective. The third limitation of the study was that the sample findings only focused on airport security, meaning that the findings cannot be generalized to other settings. However, the findings are applicable to the population of aviation and airport security.

Delimitations

The problem that was investigated is how and why the TSA chose to use the current airport security system, as it has been described by patrons and colleagues as being inefficient. Therefore, this study only focused on how and why the TSA chose the current airport security system. No other phenomena were explored in this study. Moreover, the target population of the study was reports, documents, and congressional hearings of experts in the field of aviation and airport security. No other population considered for this study. Data was collected from secondary sources. The researcher did not use any other data collection form.

Ethical Assurances

Before conducting actual data collection, the researcher first asked permission from the Northcentral University IRB. There were no human subjects in this study. The researcher used secondary data, consisting of public documents, to conduct this study. The researcher kept all physical data electronically secured. The researcher stored all physical data sheets and other physical documents related to the study inside a locked cabinet in her personal home office. The researcher saved and stored all electronic documentations in a password protected personal laptop that was only used for this dissertation. The researcher secured all the files with a password. After completing the dissertation, the researcher will continue storing these documents and data in their respective storage for five years. After the five years, the researcher will destroy all data though shredding or permanent deletion.

Summary

The purpose of this qualitative single case study was to explore the operations of the TSA in terms of resource allocation and the extent to which it uses or should use a risk-based approach allocation system. The researcher gathered reports and documents from the GAO, TSA, and Congressional Hearings. The Colaizzi (1978) seven-step method assisted the researcher with the proper guidance to stay on course and execute steps to ensure that a concentrated and comprehensive investigation was conducted. A thematic method was used to analyze data. The NVivo software aided the researcher in managing and investigating patterns found in the data. The use of the NVivo software assisted with cementing the creditability of data findings that were acknowledged and tested.

Chapter 4: Findings

This qualitative research analysis composed of two sub-case studies: TSA operations from the prospective of the Government Accounting Office (GAO) and TSA operations from the perspective of congressional hearings in response the three research questions developed for this research study. There were 19 documents that were analyzed and coded using NVivo 12 software. The NVivo software was used to process the large amount of textual data from the documents and reports gathered in the data collection phase. Specifically, the researcher used NVivo software to code the data and group the codes into themes that were relevant to the topic and research questions. The research questions and sub-questions developed for this study were as follows:

RQ1: How does the TSA decide on efficient airport security systems and how do they adapt their airport security systems?

RQ2: How does the GAO impact the TSA's decision on airport security systems?

RQ3: How do the Congressional hearings impact the TSA's decision on airport security systems?

The inclusion criteria of the documents were the following areas of inquiry: costs, benefits, known risks, and decision-making, as described in detail in the previous chapters. Purposive sampling was the method for deciding which documents should be included in the data set for analysis to ensure that the documents were most likely to belong within the boundaries of the afore mentioned inclusion criteria

Trustworthiness of Data

The research questions were explored using secondary data since primary data were not able to be collected via interviews of either senior TSA officials or members of Congress. Therefore, the population for the current study was the Government Accounting Office (GAO)

reports and congressional hearings regarding TSA operations. These data sets were available online and accessible to the public. The data collected from the GAO and congressional hearings were trustworthy because the reports and documentation used for this study consisted of sworn testimonies under oath. The data were also investigated by the GAO, an organization tasked to conduct oversight, review, evaluate, and fund disbursements of various government entities, including the TSA.

There was a constant comparative approach to analyze data for this study. When performing the constant comparative method of analysis, there were three major phases of coding: open coding, axial coding, and selective coding (Fram, 2013; Olson, McAllister, Grinnell, Walters, & Appunn, 2016). While performing the readings, text was broken into small segments by determining only those that were relevant to addressing the research questions of the study. From these segments, the coding system for the analysis of the entire data set was devised (Fram, 2013). Next, axial coding connected the codes into meaning groups (Fram, 2013). Possible groupings of the codes were identified and relationships between the groups of data recognized. For this study, the common emergent themes formed the major areas of inquiry: costs, benefits, known risks, and decision-making. Data were also coded for examples of effectiveness, efficiency, and inefficiency. The tree-map represented the hierarchy coding analysis, as seen in Figure 1.

Figure 1. *Tree-map of the hierarchy coding analysis*.

Results by Research Questions

In response to the overarching question about how the operations of the TSA could be made more efficient and enhance airport security, and comparing the GAO reports to the congressional hearings, the analysis found that the GAO identified known risks, decision-making, costs, benefits, and recommendations in more detail and at a higher rate than the congressional hearings did. The congressional hearings identified known risks as the main theme in response to the research question and provided recommendations, but also focused on protecting whistleblowers.

Overall, 63% of documents discussed aspects of effectiveness as compared to 32% of the documents that were coded for inefficiency, as seen in Table 1. However, when comparing the frequency of references reporting inefficiency to the effective and efficient aspects of TSA operations, there were slightly more references to inefficiencies than to efficiency or effectiveness. There were 31 references coded for inefficiency and 30 references coded under the themes of effective and efficient. The themes detailed below include details reporting what operations were effective and what was inefficient. The descriptions of all themes are included in

the codebook as well as frequency of references across the number of files coded for that theme in NVivo.

Table 1. *Codebook (Overall Study Themes)*

Theme	Description	Files	References
Assessment Needed	measurement, evaluation, testing of processes, physical structures, perimeters, or accuracy	12	51
Unreliable Assessment	measurement, calculations, and specs were not able to be depended on to be accurate	4	18
Benefits	positive outcomes for aviation and security processes, aviation and airport employees, and/or for passengers	8	43
Cost	financial output	5	17
Decision-Making	process of determining and/or the people who are in the position to determine processes including choices for finance, resources allocation, use of technology, security procedures, hiring employees, and monitoring all security operations	7	51
Effective	positive outcomes for safety, positive perceptions of safety, accurate screening for safety	10	25
Efficient	timely processes for safety screening	2	5
Ineffective	information on effectiveness not provided or inaccurate; deterrence difficult to measure; limited reliability or unreliable data on effectiveness	6	31
Known Risks	human errors, insider threats, and general vulnerabilities in the system warrant changes in the decision-making process	10	84
Recommendations Congress	recommendations from congressional hearings	1	5
Recommendations GAO	recommendations from GAO	10	20

RQ1: How does the TSA decide on efficient airport security systems and how do they adapt their airport security systems?

There were four key findings from the GAO data: the GAO 1) indicated a need to address known risks, which included human errors, insider threats, and general vulnerabilities, in the system that warranted changes in the decision-making process; 2) indicated that TSA had not systematically analyzed potential cost and effectiveness tradeoffs across the entire system of aviation security countermeasures; 3) reported that benefits of the operations included improved collaborative international security, centralized training, and expedited screening for some passengers; and 4) called for new types of assessment or improvements. These findings arose from analyzing the frequency of data coded under these themes from purposeful sampling of GAO reports.

Theme One: Known Risks

The largest amount of data about the TSA operations from the perspective of the GAO were coded with the theme of known risks which included human errors, insider threats, and general vulnerabilities in the system that warranted changes in the decision-making process. Fifty-three percent of the overall documents included concerns about known risks, including those in the decision-making process for the operations of the TSA. There were 84 references coded for known risks across those documents. Known risks was the most prevalent theme in both the GAO and congressional data. Forty-six percent of the congressional data were dedicated to known risks. The GAO data are included at the beginning of this section, followed by examples of known risks coded in the congressional hearing data. The description of risk analysis from the GAO data was described:

> TSA uses a risk-informed approach to schedule foreign airport assessments across all foreign locations, including Cuba. TSA defines risk as a function of threat, vulnerability, and consequence. The agency uses various data sources to assess the likelihood of a location being targeted by bad actors, the protective measures in place to prevent an attack, and the impact of the loss from a potential attack. TSA categorizes airports into three risk tiers, with high-risk airports assessed more frequently than moderate and low risk airports. (Actions Needed to Better Identify, 2018, p. 11)

Since its implementation, Secure Flight has changed the categorization and process for known risk identification. Specifically, the document, "TSA Has Taken Steps to Improve Oversight of Key Programs, but Additional Actions Are Needed" (2015), noted that:

> In 2009, Secure flight was program that identified passengers as high risk solely by matching them against federal government watch lists—primarily the No Fly List, comprised of individuals who should be precluded from boarding an aircraft, and the Selectee List, composed of individuals who should receive enhanced screening at the passenger security checkpoint—to one that uses additional lists and risk-based criteria to assign passengers to a risk category: high risk, low risk, or unknown risk. (p. 6)

In regard to the risk categories, there were data that described the formulaic approach in "TSA's Managed Inclusion Process Expands Passenger Expedited Screening, But TSA Has Not Tested Its Security Effectiveness" (2015):

> The result is that passengers associated with some data combinations that carry more risk are randomly excluded from expedited screening more often than passengers associated with other data combinations. TSA's assessment indicated that combinations of certain data elements are considered relatively more risky than other data groups and passengers

who fit this profile for a given flight should seldom be eligible for expedited screening, while combinations of other data on a given flight pose relatively less risk and therefore passengers who fit these combinations could be made eligible for expedited screening a majority of the time. (p. 11)

While TSA has tested the security effectiveness of each of these layers of security, TSA had not yet tested the security effectiveness of the overall Managed Inclusion process (as it functioned as a whole. The GAO explained in 2013:

> TSA had not demonstrated that behavioral indicators can be used to reliably and effectively identify passengers who may pose a threat to aviation security…TSA did not randomly select airports to participate in the study, so the results were not generalizable across airports. TSA collected the validation study data unevenly and experienced challenges in collecting an adequate sample size for the randomly selected passengers, facts that might have further affected the representativeness of the findings. (TSA's Managed Inclusion Process Expands Passenger Expedited Screening, But TSA Has Not Tested Its Security Effectiveness, 2016, p. 17)

The GAO reported other incidences of known risks in December 2011. They reported that:

> Limitations in TSA's criminal history checks increased the risk that the agency was not detecting potentially disqualifying criminal offenses as part of its Security Threat Assessments for airport workers…Its ability to review applicant criminal history records was often incomplete due to its status as a noncriminal justice agency….TSA and FBI had not assessed whether a potential security risk in TSA's Security Threat Assessment

process could exist as a result. (TSA Has Taken Steps to Improve Vetting of Airport Workers, p. 0)

Another example of human error as a known risk was found in regional variation. The data indicated that GAO found that during fiscal years 2012–2016 there was considerable regional variation among last point of departure airports in the level of compliance with select International Civil Aviation Organization security standards and recommended practices. The TSA attributed this regional variation to lack of airport resources or technical knowledge, among other factors. In 2013, the TSA established a working group to evaluate ways to better integrate risk management in the foreign airport assessment and air carrier inspection programs. This working group developed a risk framework, which, according to TSA documentation:

> Provides a systematic approach for analyzing risk at international airports, supports OGS decision making, and informs efforts to mitigate security deficiencies. In 2015, OGS created the ARM Directorate, which formalized the risk mitigation responsibilities of the working group and serves as the data analysis and evaluation arm of OGS. OGS officials stated that ARM helps the program focus its resources based on risk. ARM analyzes and prioritizes activities, such as training, that are designed to mitigate security vulnerabilities at foreign airports. (TSA Strengthened Foreign Airport Assessments and Air Carrier Inspections, but Could Improve Analysis to Better Address Deficiencies, 2017, p. 12)

In September 2014, the GAO also found that there were:

> Three issues affecting the effectiveness of TSA's Secure Flight program—(1) the need for additional performance measures to capture progress toward Secure Flight program goals, (2) Secure Flight system matching errors, and (3) mistakes screening personnel have made in implementing Secure Flight at the screening checkpoint. (TSA Is Taking

Steps to Improve Expedited Screening Effectiveness, but Improvements in Screener Oversight Are Needed, 2016, p. 9)

Another known risk was identified as ineffective technology and human error in regard to the operators' ability in the screening process. The "TSA Is Taking Steps to Improve Expedited Screening Effectiveness, but Improvements in Screener Oversight Are Needed" reported that:

> TSA performance assessments of certain full-body scanners used to screen passengers at airports did not account for all factors affecting the systems. The effectiveness of Advanced Imaging Technology (AIT) systems equipped with automated target recognition software (AIT-ATR)—which displays anomalies on a generic passenger outline instead of actual passenger bodies—relied on both the technology's capability to identify potential threat items and its operators' ability to resolve them. (2016, p. 7)

Data coded for known risks included human error, as evidenced by the following example from "TSA Is Taking Steps to Improve Expedited Screening Effectiveness, but Improvements in Screener Oversight Are Needed Secure Flight":

> In September 2014, we found that TSA lacked timely and reliable information on all known cases of Secure Flight system matching errors, meaning instances where Secure Flight did not identify passengers who were actual matches to these lists. (2016, p. 5)

Another known risk was reported about incomplete and unreliable testing data. Specifically, the GAO found that:

> TSA's ability to fully evaluate TSO performance in screening passengers and baggage for prohibited items is constrained by incomplete and unreliable testing data and a lack of data analysis. TSA officials also stated they do not systematically analyze test results to determine any national trends for informing future TSO training. TSA determined that

pass rate data for one of its covert testing programs that uses role players at airports to assess TSO performance was unreliable. Specifically, testing by an independent contractor indicated that TSA's covert testing data likely overstated TSO performance. TSA is taking action to determine the root cause of the variance in the testing results and is implementing corrective actions. TSA does not track the implementation, where appropriate, of recommendations made based on the covert testing results. (TSA Is Taking Steps to Improve Expedited Screening Effectiveness, but Improvements in Screener Oversight Are Needed, 2016, p. 0)

Within the theme of known risks were data that described hardware and software insufficiencies as well as human error in performance. For example,

Recent covert tests conducted by the DHS-OIG highlighted the following areas of concern: (1) the effectiveness of the passenger screening process, (2) TSA's Advanced Imaging Technology (AIT) screening equipment, (3) related automated target recognition software used by the AIT systems, and (4) checkpoint screener performance in identifying and resolving potential security threats at airport checkpoints. TSA lacks assurance that (1) the decisions it makes on the content of the TIP image library are fully informed, and (2) TSOs are receiving remedial training from the TIP program which has been developed to aid their ability to identify prohibited items. (TSA's Managed Inclusion Process Expands Passenger Expedited Screening, But TSA Has Not Tested Its Security Effectiveness, 2015, p. 7)

In coding the congressional transcript data, the large majority of the data were coded for the known risks theme. Forty-Six percent of the data from Congress were identified as known risks. The congressional report identified the need for urgent reforms in security operations to

help ensure the safety of the American people in terms of known risks. Specifically, regarding its report on known risks as it pertained to air marshals:

> The Inspector General's unclassified summary did not discuss specific findings, but it did have the following unclassified title: FAMS' Contribution to Aviation Transportation Security is Questionable. With respect to the air marshal program's ability to deter attacks, the unclassified version of the report warned: TSA does not have information on its effectiveness in doing so, nor does it have data on the deterrent effect resulting from any of its other aviation security countermeasures (Urgent Reforms Needed at TSA, 2018, p. 4).

The data from the Congressional hearings also went into details about the need to protect whistleblowers who identified areas of known risks including unreliable assessments and other assessments needed. In March 2017, Inspector General Roth testified at a Committee hearing regarding the potential security impacts of TSA's arbitrary personnel practices in response to questions from Rep. Brenda Lawrence:

> Rep. Lawrence: Inspector Roth, do arbitrary personnel practices deter whistleblowers from speaking out about security deficiencies?
>
> Inspector General Roth: I believe that it's got a chilling effect. Any time there is the threat of some sort of improper personnel practice as a result of making a protective disclosure, for example, of a safety situation or other kind of misconduct on the part of the agency, that there is always that fear that there is a chilling effect that something will happen to that person.
>
> Rep. Lawrence: So if TSA employees are reluctant to raise these deficiencies they observe, couldn't this put aviation security at risk?

Inspector General Roth: Well, that's absolutely the case (Urgent Reforms Needed at TSA, 2018, p. 6).

Theme Two: Cost

Of the 19 documents, 26% discussed the costs related to the TSA operations. Since the attacks of September 11, 2001, the TSA has spent billions of dollars on aviation security programs. The data from the GAO explained that $106 million had been spent on training and transformation of security officers. The GAO reported:

> Since 2016, TSO Basic Training—initial training for newly hired TSOs, including both TSA-employed and private screeners—has consisted of an intensive two-week course at the TSA Academy located at FLETC. TSA has obligated about $53 million for the program from its inception through March 2018. Of the $53 million obligated from January 2016 through March 2018, TSA obligated $18.2 million for procurement and development of the modular buildings on the FLETC campus used for TSA training, as well as associated hardware and set-up obligations such as audio/video equipment and fully operational simulated checkpoints. TSA obligated an additional $12 million in fiscal year 2016 and $13.7 million in fiscal year 2017 for the delivery of TSO Basic Training, including associated student travel and related equipment. TSA officials told us that due to continuing budget resolutions that funded the government between October 2017 and March 2018, TSA was not able to fully fund the interagency contract between TSA and FLETC to support the TSO Basic Training course in fiscal year 2018 at the beginning of the year. For this reason, TSA does not yet have 2018 training obligations available for reporting through its accounting system. However, based on the average cost per student in fiscal year 2017 of about $2,300 to attend TSO Basic Training, TSA estimates total

training obligations of approximately $9.1 million in the first half of fiscal year 2018. (Basic Training Program for Transportation Security Officers Would Benefit from Performance Goals and Measures, 2018, p. 7)

A concern about cost was included in the GAP data when it was stated that the TSA has not systematically analyzed potential cost and effectiveness tradeoffs across the entire system of aviation security countermeasures. Due to this, the GAO reported:

> TSA should continue to limit future funding for its behavior detection activities until it can provide such evidence. For FAMS—a program that deploys armed law enforcement officers on certain flights at an annual cost of about $800 million for fiscal year 2015—officials reported that one of the primary security contributions is to deter attacks. (Actions Needed to Systematically Evaluate Cost and Effectiveness Across Security Countermeasures, 2017, p. 0)

There were also penalties recorded and coded for costs associated with the operations of the TSA. The GAO wrote in air cargo:

> TSA conducted investigations covering the 548 potentially more serious violations, which resulted in about 220 administrative actions, nearly 50 civil penalties, and over 30 instances where no action was taken. According to TSA, TSA inspectors recommended total civil penalties of approximately $23.5 million, $22.2 million of which consisted of penalties proposed for one air carrier. (TSA Uses a Variety of Methods to Secure U.S.-bound Air Cargo, but Could Do More to Assess Their Effectiveness, 2018, p. 18)

The congressional hearing only discussed cost in regard to settlements and compensatory damages. Specifically, testimony mentioned,

> In May of this year, the Office of Special Counsel (OSC) announced that it had obtained a settlement with TSA on behalf of three agency employees who were given directed reassignments that required them to move from Hawaii to the U.S. mainland "after making disclosures related to airport operations and safety." The settlement included "compensatory damages of approximately $1 million" and required TSA to reassign the two individuals still employed by the agency back to their previous duty stations. (Urgent Reforms Needed at TSA, 2018)

Theme Three: Benefits

Some of the benefits of TSA operations that were reported included training, new programs for expedited screening, and an increase in the number of joint airport assessments with the European Commission. The GAO described the benefits of the TSA operations in regard to basic training:

> The (TSA) established the Transportation Security Officer (TSO) Basic Training program at the TSA Academy at the Federal Law Enforcement Training Centers (FLETC) in Glynco, Georgia to obtain benefits from centralized training. Prior to the Basic Training program, TSO training was conducted at individual airports, often by TSOs for whom instruction was a collateral duty. According to a business case developed by TSA for Congress in 2017 and TSA officials, TSA expected implementation of the TSO Basic Training program to provide efficiencies to the delivery of new hire training for TSOs and to enhance the professionalism and morale of newly hired screeners. TSO Basic Training facilities have airport checkpoint equipment and X-ray image simulators for students to practice skills, eliminating the challenge of finding available equipment and

training times in a busy airport environment. (Basic Training Program for Transportation Security Officers Would Benefit from Performance Goals and Measures, 2018, p. 0)

According to program officials, centralized training also provides trainees with an increased focus on the TSA mission and instills a common culture among TSOs. The GAO described:

> The anticipated benefits identified generally align under two distinct categories: (1) efficiencies and improvements obtained through the centralized delivery of training, and (2) enhanced professionalism and "esprit de corps" obtained through bringing newly hired screeners together for centralized training. Collectively, these benefits were also envisioned by TSA headquarters officials to have a positive impact on screening effectiveness and public perception of the TSA workforce. (Basic Training Program for Transportation Security Officers Would Benefit from Performance Goals and Measures, 2018, p. 8)

There were benefits to the passengers too. As part of TSA Pre✓™, a 2011 program through which TSA designated passengers as low for expedited screening, TSA began screening against several new lists of pre-approved low-risk travelers. TSA also began conducting TSA Pre✓™ risk assessments, an activity distinct from matching against lists that uses the Secure Flight system to assign passengers scores based upon their travel-related data, for the purpose of identifying them as low for a specific flight. The GAO data described how TSA began providing expedited screening to selected passengers and had expanded the availability of such screening to increasing numbers of passengers as part of its overall emphasis on risk-based security. For example,

Passengers who qualify for expedited screening enjoy varying levels of benefits, including not having to remove their shoes, light outerwear, jackets, belts, liquids, gels and laptops for X-ray screening at airport security checkpoints.

By determining passenger risk prior to travel, TSA intended to focus its screening resources on higher-risk passengers while expediting screening for lower-risk passengers. (TSA Has Made Progress Implementing Requirements in the Aviation Security Act of 2016, 2017, p. 4)

Another benefit was that the TSA has increased the number of joint airport assessments with the European Commission. Specifically, the foreign airport data indicated:

TSA officials GAO met with indicated that TSA's strong relationship with the European Commission has afforded the agency excellent access to foreign airports in Europe and a better understanding of vulnerabilities at these locations, which has resulted in more comprehensive assessments. (TSA Strengthened Foreign Airport Assessments and Air Carrier Inspections, but Could Improve Analysis to Better Address Deficiencies, 2017, p. 14)

Theme Four: Assessment Needed

Of the documents, 63% of the documents were coded for the theme of the need for assessment, with 51 references about the need for new types of assessment or improvements. There were 15 references about assessment needed in the GAO recommendations. One-third of the recommendations from the congressional hearings were about assessment needed to resolve security issues.

The GAO made recommendations, including that TSA update its risk assessment of airport security, develop and implement a method for conducting a system-wide assessment of

airport vulnerability, and update assessment to reflect changes in the airport security risk environment. TSA has made progress in assessing risks to airport security, but limitations remained in updating assessments, assessing system wide vulnerability, and monitoring trends. GAO noted:

> TSA has not updated its risk assessment of airport perimeter and access control security or shared updated risk information with stakeholders. While TSA released its Risk Assessment of Airport Security in May 2013, it has not updated this assessment to reflect changes in the airport security risk environment or routinely shared updated national risk information with airports or other stakeholders. TSA has not assessed vulnerability of airports system-wide. (Airport Perimeter and Access Control Security Would Benefit from Risk Assessment and Strategy Updates, 2016. p. 0)

The GAO recommended that the TSA develop and implement a method for conducting a system-wide assessment of airport vulnerability that would provide a more comprehensive understanding of airport perimeter and access control security vulnerabilities. Specifically, they recommended to,

> Use security event data for specific analysis of system-wide trends related to perimeter and access control security to better inform risk management decisions; explore and pursue methods to assess the deterrent effect of TSA's passenger aviation security countermeasures, with FAMS as a top priority to address; and for BDA—a program to identify potential threats by observing passengers for behaviors indicative of stress, fear, or deception—in July 2017, GAO reported that TSA does not have valid evidence supporting most of its behavioral indicators. (Airport Perimeter and Access Control Security Would Benefit from Risk Assessment and Strategy Updates, 2016, p. 42)

Data were coded for the need for new types of assessment in key programs to reflect new program functions as they pertained to levels of risk for different passengers. The data from GAO called for additional program measures by reporting,

> In September 2014, we found that Secure Flight had established program goals that reflect new program functions since 2009 to identify additional types of high-risk and also low-risk passengers; however, the program performance measures in place at that time did not allow TSA to fully assess its progress toward achieving all of its goals. (TSA Is Taking Steps to Improve Expedited Screening Effectiveness, but Improvements in Screener Oversight Are Needed, 2016, p. 6)

There was also a need for improved assessment as measures were considered for aviation security of foreign planes and airports. The GAO explained in "TSA Has Not Evaluated the Effectiveness of its Air Carrier Cargo Inspections or the Cargo Portions of Foreign Airport Assessments" that,

> TSA's performance measures do not allow it to specifically determine the effectiveness of its efforts to secure U.S.-bound air cargo. For example, TSA measures whether foreign airports take actions to address all noncompliance issues identified during airport assessments, but such a broad measure could obscure progress made in resolving cargo-specific vulnerabilities. Developing and monitoring outcome-based performance measures that separately account for cargo noncompliance issues and violations could help TSA better determine the extent to which its foreign airport assessments and air carrier inspections improve the security of U.S.-bound air cargo. (2017, p. 24)

The congressional hearing document also included data about the need for assessment for the effectiveness and efficiency of the TSA operations. Specifically, the congressional testimony

stated the need to "assess TSA's covert testing program to determine whether it is being fully utilized and integrated into relevant decision-making process" (p. 5).

Of the total documents, 21% were coded for noting examples of unreliable assessment within the TSA. The unreliable assessment was due to errors and at times, a lack of data. For example, the GAO reported:

> 2015 SNA data were not reliable for the purpose of reporting explosives detection canine teams' covert testing pass rates. Specifically, in the course of our review we found that these data included duplicate entries and errors, and TSA had not demonstrated that BDOs could consistently identify the behavioral indicators and, further, that decades of peer-reviewed, published research on the complexities associated with detecting deception through human observation also called into question the scientific basis for TSA's behavior detection activities. (Actions Needed to Systematically Evaluate Cost and Effectiveness Across Security Countermeasures, 2017, p. 14)

The GAO also reported that while the TSA had methods to measure its effectiveness in detecting and disrupting threats, the agency had no such methods to measure progress toward its goal of deterring attacks on the U.S. aviation system. Furthermore, there were unreliable assessments due to external factors such as the following:

> Although external factors, including host government deferrals and flight schedule data, are outside of TSA's control, TSA officials acknowledged that a tool that better corroborates and validates the flight schedule data it uses to track air carriers requiring inspection each fiscal year would improve the reliability of these data and help TSA ensure air carrier inspections in Cuba occur at the frequency established in its standard operating procedures. (Actions Needed to Better Identify, 2018, p. 14)

There were also unreliable assessments in the Secure Flight program. In September 2014, the GAO found that the TSA lacked timely and reliable information on all known cases of Secure Flight system matching errors, "meaning instances where Secure Flight did not identify passengers who were actual matches to these lists" (TSA Has Taken Steps to Improve Oversight of Key Programs, but Additional Actions Are Needed, 2015, p. 6). There were additional issues in that same report which mentioned that while the TSA used TSO screening performance data, it was constrained by incomplete and unreliable data and a lack of data analysis and assessment follow-up, and a lack of national analysis limit TSA's ability to assess TSO performance. TSA determined that ASAP pass rate results data were unreliable, which caused them to question the extent to which ASAP tests accurately measure TSO performance.

Theme Five: Effectiveness

As mentioned at the beginning of the chapter, there was almost an equal number of references for ineffectiveness as effectiveness of the TSA security operations. Overall, there 63% of documents discussed aspects of effectiveness as compared to 32% of the documents that were coded for inefficiency, as seen in Table 2.

Table 2. Excerpts from Codebook on the Effectiveness of TSA Security Operations

Name	Description	Files	References
Effective		10	25
Efficient		2	5
Ineffective		6	31

The comparison diagram shown in Figure 2 provided a visual that represented the files that were coded for effectiveness and ineffectiveness. The diagram indicated that there were 10 files that were coded for effectiveness. Four of those were also coded for ineffectiveness.

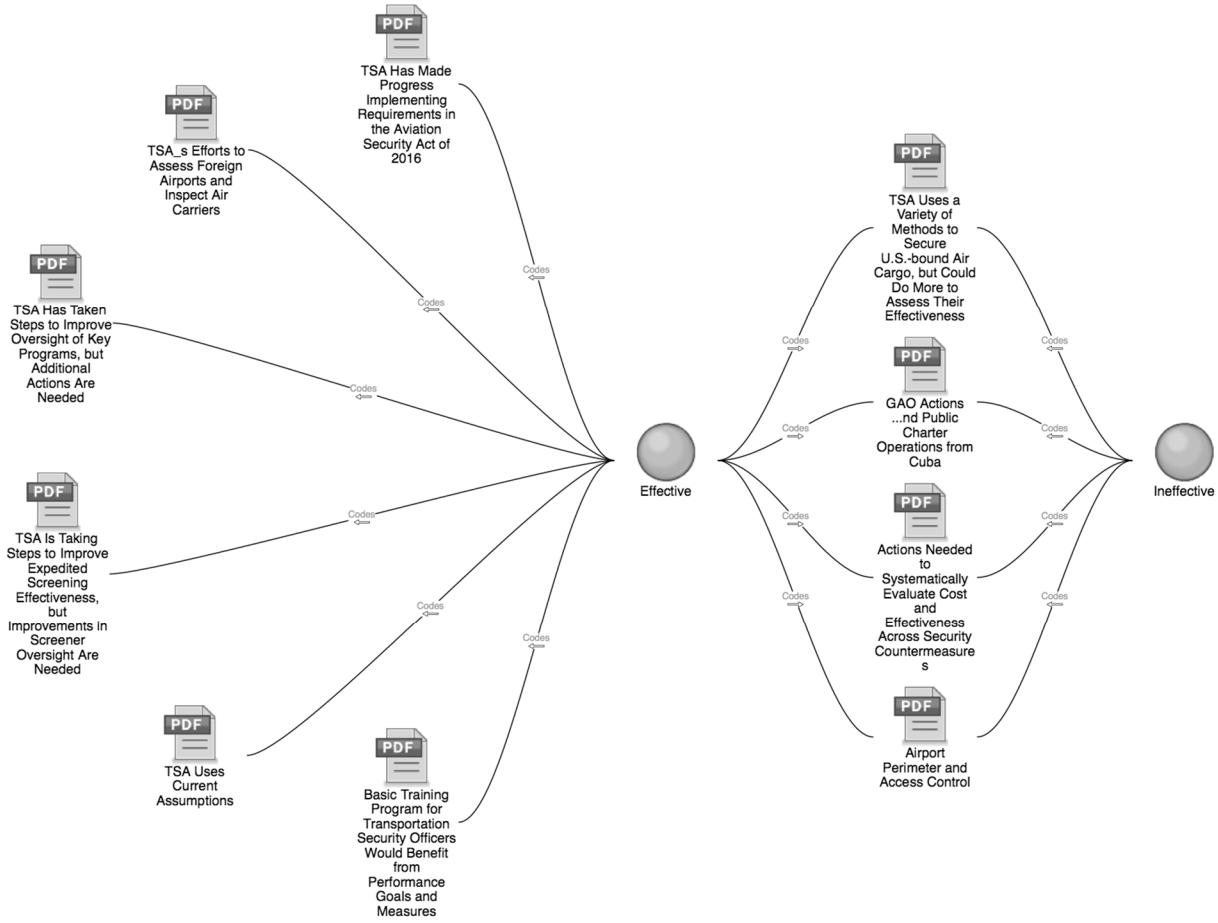

Figure 2. *Comparison diagram of effectiveness*.

To complement the comparison diagram analysis, it was important to analyze the actual amount of data coded for effectiveness as compared to ineffectiveness. The analysis that compared the frequency of references provided a better granular view of the data. Specifically, when comparing the frequency of references reporting inefficiency to effective and efficient aspects of the TSA operations, there were slightly more references to inefficiencies than to

efficiency or effectiveness. There were 31 references coded for ineffectiveness and 30 references that were coded under the themes of effective and efficient as seen in Table 1.

An example of data coded for ineffectiveness was reported in "Actions needed to systematically Evaluate Cost and Effectiveness across Security Countermeasures." It noted, "data on effectiveness of selected countermeasures in detecting and disrupting threats to aviation security vary in extent and reliability" (2017, p. 8). Another example of data coded for ineffectiveness follows:

> TSA had not demonstrated that BDOs could consistently identify the behavioral indicators and, further, that decades of peer-reviewed, published research on the complexities associated with detecting deception through human observation also called into question the scientific basis for TSA's behavior detection activities. (p. 9)

There were many examples of effective aspects of the TSA security operations. The GAO included the following example of effectiveness in "TSA's Managed Inclusion Process Expands Passenger Expedited Screening, But TSA Has Not Tested Its Security Effectiveness" when the GAO reported that, "TSA developed the Managed Inclusion process, designed to provide expedited screening to passengers not deemed low prior to arriving at the airport" (2015, p. 3).

Another document coded for effectiveness was "TSA Strengthened Foreign Airport Assessments and Air Carrier Inspections, but Could Improve Analysis to Better Address Deficiencies" where the GAO reported,

> 28 percent of passengers nationwide received expedited screening were issued TSA PreüTM boarding passes but were provided expedited screening in a standard screening lane, meaning that they did not have to remove their shoes, belts, and light outerwear, but they had to divest their liquids, gels, and laptops. (2017, p. 2)

RQ2: How does the GAO impact the TSA's decision on airport security systems?

In response to the second research question there was one theme that emerged from the analysis of the data. The GAO asserted there is a need to address the process of decision making. The GAO uncovered examples of decisions being made without integrating perspectives from primary stakeholders. The GAO also found that the TSA did not have relevant and appropriate data to make sound decisions.

Theme One: Decision-Making

Decision-making was one of them most important topics in the GAO documents, making up 37% of the data from 47 references coded. One of the primary examples of decision-making impacting the effectiveness of TSA operations was explained in the following data about a decision to allow small knives and certain sporting equipment on aircraft. Specifically, TSA did not effectively solicit feedback on its 2013 PIL decision from relevant external stakeholders, some of who subsequently expressed strong opposition to the decision to remove small knives from the PIL. The GAO has previously recommended:

> TSA strengthen its evaluation methods for operationally testing proposed modifications to checkpoint screening procedures, including changes to the PIL. However, TSA has not consistently implemented this recommendation. Conducting additional risk analysis would have allowed TSA to actually measure whether airport screeners would be better able to identify explosives if they no longer had to screen for small knives. For example, prior to announcing its decision, TSA did not coordinate with or obtain input from the Aviation Security Advisory Committee, which is TSA's primary external advisory group for aviation security matters and whose membership includes various airline industry associations. Some relevant stakeholders, such as flight attendant groups—from whom

TSA did not adequately solicit feedback— subsequently expressed strong opposition to the proposal, which contributed to TSA reversing its decision to implement the change after having already trained screening personnel for its implementation. Having a defined process and associated procedures in place to communicate with relevant stakeholders earlier in the decision-making process could allow TSA to ensure appropriate consideration of their perspectives in the decision-making process. Use of a defined process and associated procedures could also allow TSA to better avoid rescission of any future changes after investing resources in training screening personnel and informing the general public of the change—as happened in the case of TSA's 2013 PIL decision.

TSA consulted both internal and external stakeholders during development of its decision to remove small knives from the PIL, but it did not adequately consult with several external aviation stakeholder groups. Some of these groups later raised strong objections after TSA publicly announced the change. TSA did not coordinate with or obtain input from the Aviation Security Advisory Committee (ASAC), which is its primary external advisory group for aviation security matters and whose membership includes various airline industry associations. Also, some relevant stakeholders—from whom TSA did not adequately solicit feedback— subsequently expressed strong opposition to the proposal. (TSA Should Take Additional Action to Obtain Stakeholder Input when Modifying the Prohibited Items List, 2015, p. 0)

The GAO data reported that while the TSA had taken steps to leverage the results of foreign airport assessments and air carrier inspections to monitor system-wide vulnerabilities and inform capacity development, the TSA still lacks key information for decision making. For instance,

> The Open Standards and Recommended Practices Findings Tool (OSFT) —a database for tracking the resolution status of identified foreign airport deficiencies—has gaps and its system for categorization does not result in sufficient specificity of information related to security deficiencies' root causes and corrective actions. (TSA's Efforts to Assess Foreign Airports and Inspect Air Carriers, 2017, p. 1)

The GAO also noted that while the TSA has taken steps to strengthen its analytical processes, a preliminary analysis showed that the TSA lacked key information for decision-making. Specifically,

> TSA's database for tracking the resolution status of security deficiencies does not have comprehensive data on security deficiencies' root causes and corrective actions. For example, GAO found that 70 percent of fiscal year 2016 records in TSA's database exhibited empty fields pertaining to root cause or recommended corrective action. (TSA's Efforts to Assess Foreign Airports and Inspect Air Carriers, 2017, p. 0)

Another problem concerning decision-making that the GAO explained was that, according to TSA officials, each airport in the United States has unique characteristics that make it difficult to apply a one-size-fits-all solution to staffing security operations. For instance,

> Officials told us that some airports are allocated additional staff to account for the time needed to transport TSOs to off-site training facilities. Because the staffing allocation resulting from TSA's model does not reflect the full range of operating conditions at individual airports, TSA headquarters officials use airport-specific information to further adjust allocations by changing individual line items within the allocation after running the model on both an annual and an ad hoc basis. TSA headquarters officials stated that they have developed methodologies for making standard line item adjustments such as

> training requirements, overtime, and annual and sick leave. Officials told us they review the methodologies each year and use their professional judgment to modify the methodologies to account for changes in airport needs as well as budget constraints. We found that through its process of tailoring staffing allocations to individual airports' needs, TSA is able to respond to the circumstances at each individual airport. (TSA Uses Current Assumptions and Airport-Specific Data for Its Staffing Process and Monitor Passenger Wait Times Using Daily Operations Data, 2018, p. 14)

The Congressional hearing data asserted that within the reformation of the TSA processes, a priority was to "assess TSA's covert testing program to determine whether it is being fully utilized and integrated into relevant decision-making process" (Urgent Reforms Needed at TSA, 2018).

RQ3: How do the Congressional hearings impact the TSA's decision on airport security systems?

The GAO and Congress both provided recommendations to make TSA operations more effective and efficient for safety operations. In comparing the recommendations, the analysis indicated the same trend that was described at the beginning of the chapter—the GAO provided more detail, depth, and breadth to their recommendations as compared to the ones from Congress. The GAO includes several recommendations that fall under the previous themes of addressing known risks, conducting comprehensive cost and benefits analysis, including all relevant stakeholders in decision-making, creating and conducting comprehensive assessment with accurate and available data, and making that data available for the decision-making process. Congressional recommendations fall under three themes: implement security operations,

strengthen personnel management to protect whistleblowers reporting safety concerns, and transparency. The GAO recommendations follow:

(1)The Administrator of TSA should explore and pursue methods to assess the deterrent effect of TSA's passenger aviation security countermeasures; such an effort should identify FAMS—a countermeasure with a focus on deterring threats—as a top priority to address.

(2)The Administrator of TSA should systematically evaluate the potential cost and effectiveness tradeoffs across countermeasures, as TSA improves the reliability and extent of its information on the effectiveness of aviation security countermeasures

(3)TSA update its Risk Assessment of Airport Security, develop and implement a method for conducting a system-wide assessment of airport vulnerability, and update its National Strategy for Airport Perimeter and Access Control Security.

(4)The Administrator of TSA should establish specific goals for the TSO Basic Training program and develop performance measures that can be used to assess if the program is achieving desired outcomes and help ensure accountability for training results on a regular basis.

(5)The Administrator of TSA should instruct the Office of Global Strategies to improve TSA's ability to identify all public charter operations requiring inspection in Cuba and develop and implement a tool that corroborates and validates flight schedule data to more reliably track air carriers' public charter operations between the United States and Cuba.

(6)The TSA and the FBI jointly assess the extent to which this limitation may pose a security risk, identify alternatives to address any risks, and assess the costs and benefits of pursuing each alternative.

(7)Airports submit complete TSO performance data, the data are analyzed nationally, and implementation of covert testing recommendations are tracked; collect complete data on assessments of X-ray machine operators; analyze these data nationally for opportunities to enhance TSO performance, and track the implementation of covert testing recommendations.

(8)Develop a mechanism for trend analysis, establish criteria and guidance to help decision makers with vulnerability ratings, and consider the feasibility of conducting more targeted foreign airport assessments and compiling best practices.

(9)TSA develop and monitor outcome-based performance measures to assess the effectiveness of (1) the cargo portion of foreign airport assessments, (2) air carrier cargo inspections, and (3) the NCSP Recognition Program.

(10)TSA take steps to ensure and document that it's planned testing of the Managed Inclusion process adheres to established evaluation design practices.

Whereas the GAO recommendations were extensive and detailed, the Congressional recommendations were broad, overarching, and few, but one did call for the needed assessment. Specifically, the Congressional testimony included the following recommendations:

(1) Security Operations: Based on the classified and unclassified information obtained by the Committee as part of its three-year investigation, Ranking Member Cummings recommends that Congress demand sustained accountability from TSA officials to finally implement unfulfilled security recommendations made by the Inspector General, GAO,

and others that have languished in some cases for years. Although many of these unimplemented recommendations are classified, Congress should launch a one-year oversight effort—including regular meetings, briefings, and if necessary, hearings—to ensure that TSA finally implements these recommendations and resolves security vulnerabilities

(2) Personnel Management: Ranking Member Cummings recommends that Congress consider legislative proposals to strengthen civil service protections at TSA to prevent retaliation against whistleblowers who report security deficiencies and to ensure that employees are not subject to arbitrary personnel actions, which ultimately degrade security.

(3) Transparency: Ranking Member Cummings recommends that Congress continue oversight and consider legislation to significantly enhance transparency regarding whistleblower claims, settlement agreements, and non-disclosure agreements.

According to the Office of Inspector General, 20 recommendations arising out of eight Inspector General Reports involving TSA remain open. In one example, eight recommendations remain open from the Inspector General's September 2017 classified report titled "Covert Testing of TSA's Screening Checkpoint Effectiveness." In addition, according to GAO's Recommendations Database, numerous recommendations regarding TSA security operations remain open, including recommendations from the following GAO reports: "Federal Air Marshal Service: Additional Actions Needed to Ensure Air Marshals' Mission Readiness," "Federal Air Marshal Service: Actions Needed to Better Incorporate Risk in Deployment Strategy," and "Aviation Security: Actions Needed to Systematically Evaluate Cost and Effectiveness Across Systematically Evaluate Cost and Effectiveness Across Security Countermeasures."

Evaluation of Findings

A constant comparative approach was used to analyze data. While conducting the constant comparative approach, three major phases of coding were used for this study: open coding, axial coding, and selective coding. The data were read and reread in the open coding phase to ensure that the data being used was appropriate and relevant for this study. In the axial coding phase, data was categorically grouped into emergent themes based on the study, and four themes were identified in this process. The four themes were cost, benefits, known risks, and decision-making. Data was also coded for examples of effectiveness, efficiency, and inefficiency.

The GAO data was more in-depth and thorough, as they are responsible for conducting comprehensive investigations on how the federal government spends taxpayers' dollars. They provide federal agencies with reliable, objective information to assist the government in saving money and working more efficiently. With that said, five key findings was found upon data analysis of GAO data: 1) there is a need to address known risks such as human errors, insider threats, and general vulnerabilities in the system that warranted changes in the decision-making process; 2) the TSA had no methodology for analyzing possible cost and effectiveness tradeoffs across the whole aviation security system, which is a countermeasure that should be implemented; 3) the benefits of operations included improved collaborative international security, centralized training, and expedited screening for some passengers; 4) that there is a need for new types of assessments or improvements. In response to the second research question the researcher found that it is imperative to address the procedures and processes of making decisions since there were examples of the TSA not having relevant and appropriate information to make sound decisions;

The analysis of the congressional hearings data revealed four key findings: 1) assessment was needed to resolve security issues; 2) the only discussion of cost was in regard to settlement and compensatory damages; 3) there was need to improve personnel management to protect whistleblowers; and 4) there was a need for operations to be conducted with transparency.

Across the board, 63% of the documents collected discussed aspects of effectiveness while 32% of the documents were coded for inefficiency. The frequency of references to inefficiency compared to effective and inefficient aspects of TSA operations were a bit more. Thirty-one references to inefficiency were made, whereas 30 references to effective and efficiency were made collectively.

Summary

These qualitative research findings were obtained by analyzing two sub-cases studied in response to the overarching question of how TSA operations could be made more effective and efficient while also enhancing airport security system. Due to the highly sensitive classification of the data needed for this study, obtaining primary data was not an option, as the participants are senior TSA officials and members of Congress and therefore are not readily available or willing to divulge data pertinent to national security. Therefore, secondary data used for this study. Data was collected from the Government Accounting Office and congressional hearings.

The purpose of this qualitative single case study was to explore the operations of the TSA in terms of resource allocation and the extent to which it uses or should use a risk-based approach allocation. The institutional and prospect theory framework provided guidance as to what collected data would be appropriate for this study. There was a total of 19 documents analyzed and coded using the NVivo software.

A constant comparative approach to data analysis was used to analyze secondary data using three phases of coding: open coding, axial coding, and selective coding. Each phase played

an important role in the collection and analysis of the data. Open coding was used to ensure appropriate data was used for this study, axial coding was used to categorize and find groupings relevant to the study, and selective coding was used after open and axial coding was completed and relevant data patterns emerged.

In response to the overarching question about how the operations of the TSA can be made more efficient and while also enhancing airport security systems, the data collected from the GAO and congressional hearings displayed an approximately even frequency, indicating the effectiveness as compared to the ineffectiveness. Overall, there were more documents discussing aspects of effectiveness as compared to documents coded for inefficiency. The data indicated there were slightly more reference to inefficiencies than that of efficiency and effectiveness. In sum, this means that there are measures that are effective but there are also just as many measures that need to be improved to be made more effective.

Chapter 5: Implications

Increased security threats, such as hostage taking, bombing, and physical attacks, have created a need for increased vigilance and renewed an academic interest in airline and airport national security threats (Lee & Jacobson, 2012; McFarlane &Hills, 2013). After September 11, 2001, the United States federal government increased the budgets of aviation security for better screening of passengers and luggage and formed the Transport Security Administration (TSA) (Edwards, 2013). While the Aviation and Transportation Security Act (ATSA) placed an emphasis on passenger and luggage screening, ATSA failed to offer risk assessments of individual airports, thereby creating misallocation of funds and financial waste (Jani, 2015; Poole, 2009; Price & Forest, 2016).

Current airport security screening consists of a combination of metal detectors and X-ray machines. However, audits have shown that these tools have been inefficient and can be subjected to a burdensome bureaucratic process (Edwards, 2013). Price and Forest (2016) stated that the existing aviation security system fails to efficiently utilize resources, thereby diminishing the TSA's effectiveness. The differences between airport infrastructure, airport access, and nonmetallic security threats have indicated that there is no successful one-size-fits-all approach to aviation security (Brown, Sinha, Scchlenker, & Tambe, 2016; Dahbur et al., 2012; Price & Forest, 2016). While the screening of luggage and passengers helps enhance security, the TSA has failed to account for airport infrastructure, thus limiting the effectiveness of screening (Dahbur et al., 2012). One way to mitigate these concerns is to focus on risk-based assessment measures that account for variations between airports (Janic, 2015). As resources for national security are limited, it is vital to use risk-based assessments to maximize resource allocation

(Pool, 2015). Unfortunately, the TSA often succumbs to political machinations that lead to resource mismanagement (Janic, 2015).

Considering these discrepancies, the problem investigated was how and why the TSA chose to use the current airport security system, as it has been criticized by both patrons and contemporaries for its inefficiencies. The TSA has failed to concentrate its resources on where security threats are most acute and to tailor security to individual airports; instead, officials have placed an emphasis on demographic groups as potential threats (Price & Forest, 2016). The lack of focus has resulted in the misallocation of the fixed TSA resources and a failure to address site-specific threats (Poole, 2015). However, some scholars have asserted that a risk-based system is more efficient and cost-effective (Wong & Brooks, 2015). Thus, there was a need to explore whether a risk-based method for airport security would better serve security requirements as opposed to the one-size-fits-all method for aviation security (Poole, 2015; Wong & Brooks, 2015).

The purpose of this qualitative single case study was to explore the operations of the TSA in terms of resource allocation and the extent to which it uses or should use a risk-based approach for resource allocation. The data sample for this study was gathered from current secondary data from the Government Accounting Office (GAO) reports and public congressional hearings regarding TSA operations. The TSA was treated as a single case with two sub-cases: TSA operations from the perspective of the GAO and TSA operations from the perspective of congressional hearings. To address both the problem and purpose of this research, three research questions were proposed: how does the TSA decide on efficient airport security systems and how do they adapt their airport security systems; how does the GAO impact the TSA's decision on

airport security systems; and how does the Congressional hearings impact the TSA's decision on airport security systems?

The methodology for the study was qualitative. A qualitative methodology was appropriate because there was a need for in-depth exploration of a phenomenon (Katz, 2015). The study also sought to answer questions of how and why (Yin, 2013). Qualitative research was also appropriate in order to capture the concerns of people's lives (Merriam, 2014). The research design was a single case study. Yin (2013) asserted that a single case study approach was warranted as there was a need to investigate a phenomenon within the actual environment, which could not be replicated in a controlled setting. The case study approach also requires strong data sets and detailed answers to gather insights that could not be obtained through quantitative means (Katz, 2015). Therefore, a qualitative case study approach was appropriate because the researcher explored the perceptions of government experts for deeper understanding of the one-size-fits-all approach and the applicability of a risk-based system for aviation security.

This study was significant for numerous reasons. Risk-based models for aviation security, such as the TSA PreCheck program and the SURE concept have been shown to increase effectiveness and efficiency (Beckner, 2015; Price & Forest, 2016; Wong & Brooks, 2015). Should the problem remain unexamined, the TSA could continue to be less effective and mismanage funds, thereby resulting in unnecessary expense, passenger delay, and decreased security (Bandyopadhyay, Sandler, & Younas, 2014). The research sought to increase the existing knowledge on the phenomenon by uncovering best practices that may have been overlooked. Terrorist methods are ever evolving, and a successful attack would have grave economic, security, and international consequences (Price & Forest, 2016; Wong & Brooks, 2015). The results of this study aimed to enhance the understanding of the existing TSA one-

size-fits-all system for resource efficiency and attempted to identify discrepancies and weaknesses that could be mitigated through a risk-based system.

Several limitations were identified in this investigation. As the study relied upon secondary data uncovered by individuals other than the researcher, there was potential that it may have been inaccurate or manipulated. Direct interviews were not considered as it was difficult to gain access to senior TSA officials or members of Congress, as they are often unable to discuss matters of national security. Therefore, the researcher assumed that the data was reputable and honest. The second limitation was that the data was incomplete, limited, or came from a partial perspective. Lastly, because the study was focused on airport security, it was limited and cannot be transferred to other settings of mass transit. This study was delimited to the use of the one-size-fits-all approach and a risk-based system and no other airport security systems.

The results of this study identified multiple themes. The uncovered themes were known risks, decision-making, costs, benefits, assessment needed, and recommendations. The data also indicated that effectiveness, efficiency, and inefficiency were also minor, yet pertinent, themes that should be explored. The analysis from the GAO data provided the following insights: 1) called to address known risks which included human errors, insider threats, and general vulnerabilities in the system that warranted changes in the decision-making process; 2) asserted the need to address the processes of decision-making since there were examples of making decisions without integrating perspectives from primary stakeholders and also that the TSA did not have relevant and appropriate data to make decisions; 3) indicated that TSA had not systematically analyzed potential cost and effectiveness tradeoffs across the entire system of aviation security countermeasures which should be done; 4) reported that benefits of the

operations included improved collaborative international security, centralized training, and expedited screening for some passengers; and 5) called for new types of assessment or improvements. The congressional hearing analysis yielded the following: 1) assessment was needed to resolve security issues; 2) the only discussion of cost was in regard to settlements and compensatory damages; 3) there was a salient need to improve personnel management to protect whistleblowers; and 4) operations must be conducted with transparency.

The remainder of this paper will focus on implications from the research, recommendations for practice, and recommendations for future research. Implications for the research will be compared to the existing literature and the theoretical foundation when applicable. Recommendations for practice will be the direct themes uncovered through the data analysis, while recommendations for future research were developed from gaps within the uncovered themes. Lastly, this study will offer a conclusion that encapsulates the paper.

Implications of Findings

The results from the study had numerous implications in the context of the literature and theoretical frameworks. The themes which were uncovered provided insight into the phenomenon. These themes were known risks, decision-making, costs, benefits, assessment needed, and recommendations. The themes of known risk, decision-making, costs, benefits, and assessment needed will be discussed in relation to the literature within Chapter 2 in the selected theoretical framework. However, the recommendations will be covered within the practical recommendations section. Lastly, the minor themes of effectiveness, efficiency, and inefficiency will also be examined. Each of the themes will be discussed broadly, rather than in terms of individual research questions. Therefore, the overall research question, how could the operations of the TSA be made more efficient and at the same time enhance airport security? Will be used during the discussion of the results.

Known risks. The first theme was known risks. Upon coding and analysis, known risks had the highest number of mentions. Known risks included human errors, insider threats, and general vulnerabilities in the system. Overall, 53% of the documents and 84 references focused on known risks in the decision-making process of the TSA.

Risk analysis and risk identification. Two important themes that contributed to known risks were risk analysis and risk identification. The TSA defines risk as a threat, a vulnerability, or consequence. Risk analysis was how the TSA relied upon a risk-informed approach when assessing airport security across locations. When identifying risks, the TSA focuses on the location, bad actors, protective measures, and the potential loss from an attack. The TSA has identified three risk tiers for airports. These are high risk, moderate risk, and low airports. Not to be confused with risk analysis, risk identification focuses on identifying threats, such as passengers who may intend to cause harm. Risk identification can come in the form of a no-fly list or the selected list, both of which assign individuals to a risk category of high, low, or unknown.

Although risk analysis and risk identification are as important as ever after 9/11, the U.S. government hastily created the TSA without including risk analysis or risk identification, enabling a misuse of allocated funds (Poole, 2015). Poole (2015) stated that risk analysis and identification were vital because of the economic principle of opportunity costs. Without risk analysis, the decision of how to allocate limited funds for elevated security could lead to unnecessary financial waste and reduced safety (Gillen & Morrison, 2015; Poole, 2015). Therefore, the literature suggested that risk analysis and identification must come from a holistic perspective (Gillen & Morrison, 2015). Maintaining a focus on risk is necessary to adapt to the ever-changing threats of terrorist attacks (Price & Forrest, 2016; Sandler, 2014).

However, the literature indicated that risk assessment for security policies and procedures can be complex and multifaceted (Poole, 2015). Therefore, scholars maintain that a one-size-fits-all approach for security is detrimental as it can increase implementation and maintenance costs (Gillen & Morrison, 2015; Lowe, 2015). Risk analysis and identification can help tighten checkpoint and baggage policies, access control of employees, and provide increased security coverage of airport perimeters (Poole, 2015).

Stewart and Mueller (2015) examined risk analysis in the context of cost per saved life, acceptable risk, cost benefit analysis, and risk communication. The authors found that the PreCheck component of airport security significantly reduced costs and increased efficiency to the screening process. Brown et al. (2016) noted that risk-based screening, specifically DARMS, could maximize resources and reduce screening time to help clear passengers at a greater rate. In a separate study, Cano et al. (2013) used the adversarial risk analysis model to help understand the terrorist actions and found that risk-based security diminishes potential attacks through randomized routines. Paté-Cornell and Cox (2014) uncovered three credible aspects of risk analysis, which were risk assessment, risk management, and risk communication. Risk analysis should incorporate lessons from near misses for informed decision-making from policymakers who could better understand the nature and scope of potential attacks (Dillon et al., 2014; Madsen et al., 2016).

The literature identified some effective risk identification programs. These programs were PreCheck, Secure Flight, and Managed Inclusion, all of which were cost and time efficient (Beckner, 2015). However, these programs were not without drawbacks, as passengers felt that it infringes on their privacy rights and contributes to racial profiling (Cavusoglu, Kwark, Mai, & Raghunathan, 2013; Deno et al., 2014). Despite these drawbacks, PreCheck lanes have achieved

their goals and have allowed the TSA to expand policies such as including the private sector for better operations and security (Beckner, 2015).

Regional Variations. Another sub theme of known risks was regional variation. The uncovered themes found within the GAO literature specified extensive regional variation and levels of compliance with select International Civil Aviation Organization security standards and recommended practices. The TSA attributed the disparity to a difference of resources and technical knowledge. In 2013, the TSA helped create a working group for increased evaluation of risk management among foreign airport assessment and air carrier inspection programs. This sub-theme created an opportunity for future research, as there was minimal literature within Chapter 2 regarding it.

Secure Flight. The results of the study also isolated the strongest known risks for additional performance measures for Secure Flight. They were Secure Flight program goals, Secure Flight system matching errors, and screening mistakes in implementing Secure Flight at screening checkpoints. Beckner (2015) noted that programs like PreCheck, Secure Flight, and Managed Inclusion were meant to reduce cost and time, especially when compared with technological innovations (Brown et al., 2016). However, these risk-based security options that focus on randomization still leave a window for would-be attackers to go through the system undetected while requiring regular passengers to undergo unneeded screening and regulation (Sakano et al., 2016). Although PreCheck and Secure Flight could help segregate low passengers and create better supported no-fly lists, potential attackers can still find ways around the security measures simply by recruiting new members who can pass through the system (de Goede & Sullivan, 2016; Sakano et al., 2016).

Ineffective Technology and Human Error. Another known risk was that technology can sometimes be an ineffective, especially when operators are poorly trained or inattentive. Vorobeychik and Letchford (2015) stated that while technology can help gather, share, and improve decision-making, the technology is also vulnerable to cyberattacks across the globe. Fox (2016) echoed the warning of cyberattacks, stating that could also affect aircraft.

Human error was also found to be a significant known risk. Human error could fail to match passengers to those on watch lists. The TSA has already come under fire for human error, as they have allowed weapons and bombs to go undetected (Berghel. 2015; Lowe, 2015). Human error also highlights the inefficiency of a one-size-fits-all approach. The literature has shown that an increased workload and longer shifts negatively affects baggage screeners and their ability to detect threats (Meuter & Lacherez, 2016). The increased security measures, coupled with an ever-growing volume of passengers, have created stress and time pressures that result in mistakes (Meuter & Lacherez, 2016). Baeriswyl et al. (2016) stated that workload of emotional exhaustion decreased job performance, and Skorupski and Uchroński (2015) noted that employee personal characteristics, the subjective nature of identification, and systemic inaccuracies can make baggage screening inefficient.

However, the TSA has attempted to mitigate these concerns. The human element has caused the TSA to reassess the decision-making process when updating aviation security policy (Greene et al., 2014). Creating more stringent instructions for employees can increase the success of PreCheck, Secure Flight, and risk-based screening (Brown et al., 2016). These fixes are anything but concrete, as de Gramatica et al. (2017) found that data for training officials to reduce human error is limited. Human error can also include air marshals. Air marshals can deter attacks, however, there is a lack of data on its effectiveness. Despite the lack of data uncovered

within the analysis portion of this paper, previous literature has offered support for the use of air marshals. Stewart and Mueller (2013b) found that the Federal Air Marshal service, the Federal Flight Deck Officer Program, and installed physical secondary barriers are all cost-efficient measures to add security.

While almost all the sub-themes were supported to some degree by the existing literature, other sub-themes lacked substantial support. One of these themes was the protection of whistleblowers who identified risks such as unreliable assessments. Another unsupported sub-theme was incomplete and unreliable testing data. The TSA has previously stated that they do not systematically conduct an analysis of TSO training. Yet when an independent contractor examined the existing data, it was uncovered that TSO performance was overstated. The final sub-theme not supported by the literature was implications with hardware and software insufficiencies. The effectiveness of the passenger screening process, TSA's advanced imaging technology and screening equipment, related automated target recognition software, and checkpoint screener performances were all found to be lacking. The minimal literature on each one of the subthemes provides options for future research.

Decision Making. The second theme, decision-making, had 47 references within the GAO documents. The study uncovered that while the TSA has attempted to mitigate poor decision making through monitoring system-wide vulnerabilities and informed capacity, the TSA still does not have enough data for adequate changes. The results indicated that the TSA has moved to a more analytical process when deciding aviation policy. Traditionally, the TSA has applied a one-size-fits-all approach to security operations, however, the results of the GAO analysis indicated that, because each airport has unique challenges, this tactic can be detrimental.

The congressional data aligned with the GAO documents with finding the best approach for decision-making.

The theme of decision-making is best discussed in the context of the theoretical frameworks. The first framework was Scott's Institutional Theory (2004; 2014). Scott posited that decision-making and managerial operations should be based upon three pillars: normative, regulative, and cultural-cognitive (Scott, 2014). Normative factors detailed how things are run, regulative acknowledges the rules, regulations, and legal elements of decision making, and cultural-cognitive features the beliefs and values that inform policymaking (Scott, 2014). These three elements differ in their influence between institutions and organizations. Scott (2014) placed a strong emphasis on social structure and how individuals make their decisions while balancing logic, facts, emotions, and cultural beliefs.

The results of the study did not outright determine which pillar had the strongest effect in aviation security decision-making. However, because of the complex nature of aviation security, regulative decision-making seemed predominant with normative being a supporting role. The lack of connection to cultural-cognitive elements is important. As both the GAO and congressional analysis indicated failures in the decision-making process, a cultural-cognitive analysis could provide further insights. Previous literature mentioned an unnecessary emphasis on racial and cultural screening. Through the cultural-cognitive lens, these policies' validity could be better assessed and understood. By placing an emphasis on screening, risk-based analysis of airport security on a case-by-case basis ends up being ignored.

The second theory that focused on decision-making was prospect theory. Prospect theory was a behavioral-economic framework that stated that risk-based decisions are often made on the chances of success and failure or gains and losses (Kahneman & Tversky, 1979). Prospect theory

concentrates on the monetary outcome through analysis of variables that can detail gains and losses (Kahneman & Tversky, 1979). There were two phases to this theory: editing and evaluation. Editing consists of evidence that is organized to help form outcomes and the evolution phase assesses the gains or losses of those outcomes. Decisions are then made on the basis of the maximum utility or benefit of the analysis (Kahneman & Tversky, 1979). Prospect theory aligns with risk analysis where the gains and losses are measured for better aviation security. Should the TSA rely upon a more risk-based approach to policymaking as mentioned within the first theme, it would be wise to use prospect theory to frame their decision-making process.

Other uncovered literature could also contribute to and enhance understanding of decision-making. Both Shafieezadeh et al. (2015) and Stewart and Mueller (2013b) found that differing combinations of security measures provide optimal aviation security. Stewart and Mueller (2013b) examined cost efficiency through physical secondary barriers, the Federal Air Marshals service, and Federal Flight Deck Officer Program to determine that the latter had the best outcomes. Shafieezadeh et al. (2015) employed a cost and benefit approach to the TSA's screening of passengers and found that video surveillance offered optimal results. Both of these studies displayed how flexible decision-making can create the best economical and proficient aviation security policy.

Decision-making for aviation security should include financial, resource allocation, technological, procedural, hiring, and monitoring practices, each of which ought to be measured by their costs, values, and hazards. Scholars differ on which element should have the most emphasis when formulating policy. Gillen and Morrison (2015) and Poole (2015) felt that allocation of funds and resources should be considered the most, while Lowe (2015) and Greene

et al. (2015) purported that human errors that came from poor hiring and training created the greatest amount of risk.

Other scholars felt that airport location should be a prime factor in decision-making. Citizens often travel to locations where they feel the safest and terrorists identify these locations as prime opportunities for an attack, even when there is little chance for success (Bausch & Zeitzoff, 2015; Garcia & Winterfeldt, 2016; Goldman & Neubauer-Shani, 2017). Decision-making for aviation security should also focus on the amount of time it takes for passengers to go through screening and if they end up feeling inconvenienced after the process (Gillen & Morrison, 2015; Stewart & Mueller, 2013a). Therefore, policymakers should find a balance between convenience and security (Scurich & John, 2014). Lastly, Paté-Cornell and Cox (2014) and Dillon et al. (2014) asserted that some of the best data for decision-making come from near misses and failed attacks. Data gathered from previous incidents can help determine weak points and where resources should be focused. As mentioned in the first two themes, cost is another important element that can determine policy.

Cost. From the 19 documents that were assessed, 26% of those documents indicated that cost was an important theme. Since 9/11, the TSA has spent over $106 million on security officer training despite not using data-driven analysis to assess the costs and effectiveness of the training. The congressional data discussed cost only in terms of settlements and compensatory damages. The literature from Chapter 2 offers further context for the importance of cost as a theme.

Each program and policy for airport and airline safety has different costs, some of which can be offset. The PreCheck program has been shown to decrease screening time and costs passengers a fee to use (Jacobson et al., 2016). PreCheck passengers are able to decrease the

waiting time for regular passengers while also providing additional funding. Isolating and analyzing the PreCheck program prevents a one-size-fits-all approach to policymaking, which is vital with the increase of passengers per year (Scurish & John, 2014). By examining policies individually, a greater assessment of cost and waste can be conducted.

As security is federally funded, it is important to minimize costs. Leese (2016) examined the outsourcing of security to private firms and found that they created increased malleability and reduced costs. Clavell (2015) noted that big data and privatization can improve airport security at a decreased cost because the private sector may have better technological resources than the public sector. Another way to reduce costs and wait time for passengers was randomization of screening. However, this process could also lead to diminished efficiency (Beckner, 2015; Brown et al., 2016; Gillen & Morrison, 2015; Lowe, 2015). Cavusoglu et al. (2013) added that profiling may have cultural costs, but they also decrease financial costs and chances of an attack. Some scholars have specified that a risk-based system is the most cost-effective way to assess aviation security. As each airport varies in size and importance, a risk-based system based on cost-benefit analysis could help reduce expenditures (Amorim da Cunha, Macário, & Reis, 2017). With risk-based analysis, both cost and benefits are assessed.

Benefits. The fourth theme, benefits, detailed the positive aspects of some of the TSA's operations. One significant benefit was Transportation Security Officer Basic Training at the TSA Academy federal law enforcement training centers. This basic training enhanced efficiency and morale of new screeners, offering security specialists better knowledge of the equipment, cultural sensitivity, and competent skills that could not be taught in a busy airport setting. Benefits were placed into categories. The first was efficiencies and improvements obtained

through the centralized delivery of training and the second was enhanced professionalism obtained through bringing new hired screeners for centralized training.

Employees were not the only ones who reaped the benefits of efficient aviation policies. Passengers also profited. For instance, the GAO data indicated that PreCheck expedited the screening process for accepted passengers and reduced the workload for screeners, allowing them to focus their attention on their job. PreCheck passengers also did not have to take off their shoes, jackets, belts, liquids, gels, and laptops during the screening process at airports. Another benefit was that the TSA could share assessments with the European commission. These assessments offered increased comprehension of vulnerabilities and attack opportunities.

The literature supported many of these findings. Becker (2015) noted that the bombing of Pan America Flight 103 helped other airports increase their screening as well as identify poor hiring and training practices. Ergün et al. (2017) pointed out the benefits of biometrics in reducing passenger stress and increasing security, and de Gramatica et al. (2017) found how specialized training was more beneficial than a one-size-fits-all approach. Beckner (2015) and Jacobson et al. (2016) supported this study's findings on the PreCheck programs as they reduced the workload for TSA employees and increased passenger satisfaction. Brown et al. (2016) added that the Secure Flight program, in conjunction with PreCheck and better technology, was also shown to be beneficial. Beckner (2016) found that the mere installation of the PreCheck program saved the TSA over $100 million in the 2014 fiscal year. However, joint airport assessment benefits were not supported within the literature from Chapter 2, thereby creating a need for future research.

Assessment Needed. The final theme was assessment needed. There were 51 references among 63% of the documents, making it a pertinent theme. The data found a need for the

assessment of existing programs to understand the degrees of risk for varying passengers. The GAO made multiple recommendations regarding assessment. The data indicated that the TSA should improve its risk assessment for AirPort Express security while developing and implementing a system-wide assessment of airport environment vulnerability. These assessments can be composed of understanding systematic vulnerabilities and monitoring trends. Assessing vulnerabilities could offer an increase understanding of airport perimeter and access deficiencies. The GAO also pointed out the need to assess the aviation security for foreign planes and airports. The congressional hearing documents specified the need to assess the TSA's decision-making process. The GAO report detailed that the TSA is lacking the measurement tools for assessment of specific vulnerabilities such as the Secure Flight program and foreign airlines.

The literature also pointed out the need for assessment. Poole (2015) stated that the hurried creation of the TSA led to a department with mismanaged funds and poorly implemented policies. Other authors noted that the hasty creation of the department was meant to assure passengers that they were in safe space; however, a lack of risk assessment and cost-benefit analysis proved that the one-size-fits-all approach was detrimental over time (Poole, 2015; Scurish & John, 2014). Assessing how terror attacks change the respondent to new security protocols also indicates a need for constant assessment (Price & Forrest, 2016; Sandler, 2014).

Effectiveness. Although not a prominent theme, effectiveness should also be examined. The results of the study yielded that ineffectiveness and effectiveness related directly to the TSA security performance. Specifically, security countermeasures for detection and disrupting threats tended to differ in their success and reliability. The GAO found that the TSA does not reliably test security effectiveness. Constant testing could improve an airport's assessment and air carrier inspections to diminish deficiencies. Effectiveness was also mentioned within the literature.

Programs such as randomized screening and PreCheck were found to be effective in terms of both time and cost to screeners and passengers, while a one-size-fits-all approach remains ineffective (Brown et al., 2016; Price & Forest, 2016). Wong and Brooks (2015) found that requiring all passengers to go through the same number of screening devices reduces efficiency and effectiveness, especially when dealing with increased numbers of passengers and operating in smaller spaces. In addition to security effectiveness, time and price must also be considered. PreCheck and dynamic aviation risk management solutions all improved the effectiveness of security measures (Brown et al., 2016). Chaterjee et al. (2015) agreed with this sentiment by stating that a multi-layered approach increased the effectiveness of airport security. Jackson and LaTourrette (2015) added that multiple approaches are effective because they can compensate for each other's weaknesses. These themes also yielded GAO and congressional recommendations. These recommendations will be discussed in the following section.

Recommendation for Practice

The results of the study also produced GAO and congressional recommendations. While many of these were uncovered sub-themes, the most pertinent findings are discussed in this section. The GAO results were more detailed compared to the recommendations from Congress. The GAO recommendations include known risks, cost-benefit analysis, relevant stakeholders in decision-making, comprehensive assessments, and increase data for decision-making. The congressional recommendations were implemented security operations, strengthen personal management to protect whistleblowers, and transparency.

GAO recommended that TSA administrators assess the effectiveness of aviation security countermeasures. The administration of the TSA should compare and contrast each of these countermeasures in terms of cost and effectiveness. The TSA should also update its risk assessment of airport security to decrease vulnerability at access points in the perimeter.

Improved training has also demonstrated improved results and should be implemented across all security positions. Other recommendations were to identify risks within existing policy, assess the costs and benefits of each alternative, and make decisions accordingly. Airports should submit TSO performance data for increased analysis and better policy formation. The TSA should also assess the effectiveness of the cargo of foreign airports assessments, air carrier cargo inspections, and the CSP recognition program. Lastly, the GAO stated that the TSA should begin to test the Managed Inclusion process to adhere to the established evaluation design practices.

There were also congressional recommendations. The first recommendation was that there needed to be accountability for their inability to fulfill security policies made by the Inspector General, GAO, and other organizations. Although many of these recommendations are classified, their implementation status should be revised and assessed. Another recommendation was that Congress should strengthen civil service protections to shield whistleblowers from punishment. Protection would allow more employees to detail potential hazards and faults within airport and airline security without fear of retaliation. Lastly, Congress needs to further conduct oversight and offer new legislation to ensure transparency, settlement agreements, and nondisclosure agreements. These recommendations were derived from the results of the data found in Chapter 4 and therefore required minimal interpretation as the improvements to aviation security were plainly laid out.

Recommendation for Future Research

There are multiple opportunities for future research. Some of these opportunities come from uncovered themes not supported within the literature, while others come from limitations of the study itself. Some of the themes were unsupported by the literature, offering point of departure for future qualitative research. These themes were regional variations, whistleblowers, complete and unreliable testing data, implications for software and hardware, and joint airport

assessment benefits. Themes such as whistleblowers, unreliable testing data, and implications for software and hardware and how they relate to risk and cost-benefit analysis in addition to the decision-making process can each be specific studies. Ideally, these would be qualitative case studies with results that can later be refined into quantitative research.

The themes of regional variations in joint airport assessment benefits are also an opportunity for future qualitative research. A multiple case study could compare and contrast findings between airports. A limitation to this study was access of participants. Therefore, future research should attempt to interview stakeholders within the decision-making process. While much of the information may be protected under confidentiality and security clearances, directly hearing from TSA administrators, employees, congressmen, and congressional aides could offer greater insight into the phenomena. Lastly, a quantitative study using cost-benefit analysis could be used to further understand the budgetary constraints as well as misappropriated funds within airport and aviation security.

Conclusions

This qualitative research sought to address the problem of how and why the TSA chose to use the current airport security system, as it has been criticized by both patrons and colleagues alike for its inefficiencies. The purpose of this single case study was to increase the understanding of the factors that impact the TSA's decision to implement airport security systems and to be aware of how the decision-making process is carried out. To address both the problem and the purpose, an overarching question asked how the operations of the TSA could be made more efficient and at the same time enhance airport security. The research project employed a qualitative methodology, a case study research design, and thematic analysis that involved coding to generate themes.

The literature review covered how the 9/11 terrorist attacks have influenced government policy for aviation and airport security. Currently, the TSA uses a one-size-fits-all approach that is not always well suited to ensure citizen safety. The TSA has begun to implement a risk-based approach, yet randomized searches have come under criticism for not respecting privacy rights, promoting racial profiling, and failing to identify security breaches (Berghel, 2015; Wong et al., 2015). Upon completing the literature review, a gap was identified due to lingering concerns about the one-size-fits-all method. Additionally, existing literature does not provide enough data to compose new policy.

There has been a lack of emphasis on human errors, common technological difficulties, and new risks. The results of the study uncovered five significant themes. These were known risks, decision-making, costs, benefits, and assessment needed. Additionally, upon data analysis, direct recommendations for policy and action were identified and highlighted. This study not only provided evidence of the problems the phenomena now faces, but also offered direct recommendations derived from the data itself. Aviation and airport security are ever-changing systems; however, using this investigation as a base, future research can provide further insights into the difficulties that the TSA currently faces.

References

Abdellaoui, M., Bleichrodt, H., & Paraschiv, C. (2007). Loss aversion under prospect theory: A parameter-free measurement. *Management Science*, *53*(10), 1659–1674. doi:10.1287/mnsc.1070.0711

Albu, C. E. (2016). Tourism and terrorism: A worldwide perspective. *Ces Working Papers*, *8*(1), 1–19. Retrieved from http://www.ceswp.uaic.ro/articles/ceswp2016_VIII1_alb.pdf

Amorim da Cunha, D., M., R., & Reis, V. (2017). Keeping cargo security costs down: A risk-based approach to air cargo airport security in small and medium airports. *Journal of Air Transport Management*, *61*, 115–122. doi: 10.1016/j.jairtraman.2017.01.003

Andrews, L., Higgins, A., Andrews, M. W., & Lalor, J. G. (2012). Classical grounded theory to analyze secondary data: Reality and reflections. *The Grounded Theory Review*, *11*(1), 12–26.

Baeriswyl, S., Krause, A., & Schwaninger, A. (2016). Emotional exhaustion and job satisfaction in airport security officers - work-family conflict as mediator in the job demands-resources model. *Frontiers in Psychology*, *7*, 663. doi:10.3389/fpsyg.2016.00663

Baker, D. M. A. (2015). Tourism and Terrorism: Terrorists Threats to Commercial Aviation Safety & Security. *International Journal of Safety and Security in Tourism and Hospitality*, *1*(12), 1–18. search.proquest.com/openview/8089d53e357617d202c15539e19ffff0/1?pq- origsite=gscholar&cbl=2035879

Bandyopadhyay, S., Sandler, T., & Younas, J. (2014). Foreign direct investment, aid, and terrorism. *Oxford Economic Papers*, *66*(1), 25–50. doi:10.1093/oep/gpt026

Barnett, A. (2015). Has successful terror gone to ground? *Risk Analysis*, *35*(4), 732–740. doi:10.1111/risa.12352

Barratt, M. J., Ferris, J. A., & Lenton, S. (2015). Hidden populations, online purposive sampling, and external validity: Taking off the blindfold. *Field Methods*, *27*(1), 3–21.

Bausch, A. W., & Zeitzoff, T. (2015). Citizen information, electoral incentives, and provision of counter-terrorism: An experimental approach. *Political Behavior*, *37*(3), 723–748. doi:10.1007/s11109-014-9289-x

Beckner, C. (2015). Risk-Based Security and the Aviation System: Operational Objectives and Policy Challenges. Center for Cyber & Homeland Security: The George Washington University. Retrieved from https://pdfs.semanticscholar.org/2528/9b4090a9d8bb98d0acab73519c65c70c5233.pdf.

Berghel, H. (2015). TSA: Mission creep meets waste. *Computer*, *48*(8), 90–94. doi:10.1109/MC.2015.227

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking: A tool to enhance trustworthiness or merely a nod validation? *Qualitative Health Research*, *26*(13), 1802–1811.

Bonfanti, M. E. (2014). From sniffer dogs to emerging sniffer devices for airport security: An opportunity to rethink privacy implications? *Science and Engineering Ethics*, *20*(3), 791–807. doi:10.1007/s11948-014-9528-x

Brown, M., Sinha, A., Schlenker, A., & Tambe, M. (2016, February). One Size Does Not Fit All: A Game-Theoretic Approach for Dynamically and Effectively Screening for Threats. In *AAAI-16* (pp. 425-431), Los Angeles, CA: University of Southern California. Retrieved from http://www-personal.umich.edu/-arunesh/Files/Other/Papers aaai.darms.camera.pdf.

Budescu, D. V., & Bo, Y. (2015). Analyzing test-taking behavior: Decision theory meets psychometric theory. *Psychometrika*, *80*(4), 1105–1122. doi:10.1007/s11336-014-9425-x

Cano, J., Insua, R., D., T., A., & Turhan, U. (2016). Security economics: An adversarial risk analysis approach to airport protection. *Annals of Operations Research*, *245*(1), 359–378. doi:10.1007/s10479-014-1690-7

Cavusoglu, H., Kwark, Y., Mai, B., & Raghunathan, S. (2013). Passenger profiling and screening for aviation security in the presence of strategic attackers. *Decision Analysis*, *10*(1), 63–81. doi:10.1287/deca.1120.0258

Chan, C. K., & Anteby, M. (2016). Task segregation as a mechanism for within-job inequality: Women and men of the transportation security administration. *Administrative Science Quarterly*, *61*(2), 184. doi:10.1177/0001839215611447

Chatterjee, S., Hora, S. C., & Rosoff, H. (2015). Portfolio analysis of layered security measures. *Risk Analysis, 35*(3), 459-475. doi:10.1111/risa.12303

Clavell, G. G. (2015). Policing, Big Data and the commodification of security. In B. v. d. Sloot, D. Broeders, & E. Schrijvers (Eds.), *Exploring the boundaries of Big Data* (pp. 89–115). bartvandersloot.nl/onewebmedia/ Verkenning_32_Exploring_the_Boundaries_of_B ig_Data.pdf#page=90

Colaizzi, P. F. (1978). Psychological research as the phenomenologist views it. In Ronald S. Valle & Mark King (eds.), Existential-Phenomenological Alternative for psychology Oxford University Press.

Cole, D. (2015). The difference prevention makes: Regulating preventive justice. *Criminal Law and Philosophy*, *9*(3), 501–519. doi:10.1007/s11572-013-9289-7

Connelly, F. M., & Clandinin, D. J. (1990). Stories of experience and narrative inquiry. *Educational researcher*, *19*(5), 2–14.

Creswell, J. W (2009). Research design: Qualitative, quantitative, and mixed methods approaches (3rd. ed.,) Thousand Oaks, CA: Sage. Retrieved from http://www.ceil-conicet.gov.ar/wp-content/uploads/2015/10/Creswell-Cap-10.pdf

Dahbur, K., Isleem, M. R., & Ismail, S. (2012). A study of information security issues and measures in Jordan. *International Management Review*, *8*(2), 71–82.

De Bruijin, M. (1999). *Moblie Africa: Changing patterns of movement in Africa and beyond*. Lei-den, Germany: Brill.

De Goede, M., & Sullivan, G. (2016). The politics of security lists. *Environment and Planning D: Society and Space*, *34*(1), 67–88. doi:10.1177/0263775815599309

De Gramatica, M., Massacci, F., Shim, W., Turhan, U., & Williams, J. (2017). Agency problems and airport security: Quantitative and qualitative evidence on the impact of security training. *Risk Analysis*, *37*(2), 372–395. doi:10.1111/risa.12607

Deno, F., Diaz, C., Lliguicota, C., Norman, D., & González, R. (2014). TSA screening procedures: A threat to privacy. *International Journal of Arts & Sciences, 7*(3), 37. Edwards, C. (2013). Privatizing the Transportation Security Administration. Policy Analysis, 1-16.

Dillon, R. L., Tinsley, C. H., & Burns, W. J. (2014). Evolving risk perceptions about near-miss terrorist events. *Decision Analysis*, *11*(1), 27–42. doi:10.1287/deca.2013.0286

Edwards, C. (2013). Privatizing the Transportation Security Administration. *Policy Analysis*, *1-16*.

Egbert, S., & Paul, B. (2015). Devices of lie detection as diegetic technologies in the "War on terror." *Bulletin of Science, Technology & Society*, *35*(3-4), 84–92. doi:10.1177/0270467616634162

Elking, I., & Windle, R. (2014). Examining differences in short-haul and long-haul markets in US commercial airline passenger demand. *Transportation Journal*, *53*(4), 424–452. doi:10.5325/transportationj.53.4.0424

Ergün, N., Açikel, B. Y., & Turhan, U. (2017). The appropriateness of today's airport security measures in safeguarding airline passengers. *Security Journal*, *30*(1), 89–105. doi:10.1057/sj.2014.41

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, *5*(1), 1–4.

Federal Aviation Administration. (2014). Calendar Year 2014 Passenger Boardings at Commercial Service Airports. Accessed. www.faa.gov/airports/

planning_capacity/passenger_allcargo_stats/passenger/medi a/cy14-commercial-service-enplanements.pdf

Fram, S. M. (2013). The constant comparative analysis method outside of grounded theory. *The Qualitative Report*, *18*(1), 1.

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report*, *20*(9), 1408.

Garcia, R. J. B., & Winterfeldt, D. (2016). Defender-Attacker decision tree analysis to combat terrorism. *Risk Analysis*, *36*(12), 2258–2271. doi:10.1111/risa.12574

Gillen, D., & Morrison, W. G. (2015). Aviation security: Costing, pricing, finance and performance. *Journal of Air Transport Management*, *48*, 1. doi: 10.1016/j.jairtraman.2014.12.005

Glaser, B. G. (1992). *Emergence vs forcing: Basics of grounded theory analysis*. Sociology Press.

Goldman, O. S., & Neubauer-Shani, M. (2017). Does international tourism affect transnational terrorism? *Journal of Travel Research*, *56*(4), 451–467. doi:10.1177/0047287516649059

Greene, F., Kudrick, B., & Muse, K. (2014). Human factors engineering at the transportation security administration. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *58*(1), 2255–2259. doi:10.1177/1541931214581470

Heaton, J. (2008). Secondary analysis of qualitative data: An Overview. *Historical Social Research*, *33*(3), 33–45. Retrieved from https://www.ssoar.info/ssoar/bitstream/handle/document/19143/ssoar-hsr-2008-no_3__no_125-heaton-secondary_analysis_of_qualitative_data.pdf?sequence=1

Jackson, B. A., & LaTourrette, T. (2015). Assessing the effectiveness of layered security for protecting the aviation system against adaptive adversaries. *Journal of Air Transport Management*, *48*, 26. doi: 10.1016/j.jairtraman.2015.06.009

Jacobson, S. H., Khatibi, A., & Yu, G. (2016). When should TSA PreCheck be offered at no cost to travelers? *Journal of Transportation Security*. doi:10.1007/s12198-016-0176-z

Janic, M. (2015). Modelling the resilience, friability and costs of an air transport network affected by a large-scale disruptive event. *Transportation Research Part A: Policy and Practice*, *71*, 1–16. doi: 10.1016/j.tra.2014.10.023

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica: Journal of the Econometric Society*, *263-291*. doi:10.2307/1914185

Katz, J. (2015). A theory of qualitative methodology: The social system of analytic fieldwork. *Méthod (e) s: African Review of Social Sciences Methodology*, *1*(1-2), 131–146.

Kirschenbaum, A., & Rapaport, C. (2017). Does training improve security decisions? A case study of airports. *Security Journal*, *30*(1), 184–198. doi:10.1057/sj.2014.39

Lee, A. J., & Jacobson, S. H. (2012). Identifying changing aviation threat environments within an adaptive homeland security advisory system. *Risk Analysis*, *32*(2), 319–329. doi:10.1111/j.1539-6924.2010. 01656.x

Leese, M. (2014). The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union. *Security Dialogue*, *45*(5), 494–511. doi:10.1177/0967010614544204

Leese, M. (2016). Governing airport security between the market and the public good. *Criminology & Criminal Justice*, *16*(2), 158–175. doi:10.1177/1748895815603772

Lopes, A. M., Machado, J. A. T., & Mata, M. E. (2016). Analysis of global terrorism dynamics by means of entropy and state space portrait. *Nonlinear Dynamics*, *85*(3), 1547–1560. doi:10.1007/s11071-016-2778-1

Lowe, K. A. (2016). Safety in the sky: Will reforming and restructuring the TSA improve our security or merely infringe on our rights? *Journal of Air Law and Commerce*, *81*(2), 291–319. scholar.smu.edu/cgi/viewcontent.cgi? article=1002&context=jalc

Lum, C., Crafton, P. Z., Parsons, R., Beech, D., Smarr, T., & Connors, M. (2015). Discretion and fairness in airport security screening. *Security Journal*, *28*(4), 352–373. doi:10.1057/sj. 2012.51

Madsen, P., Dillon, R. L., & Tinsley, C. H. (2016). Airline safety improvement through experience with Near?Misses: A cautionary tale. *Risk Analysis*, *36*(5), 1054–1066. doi:10.1111/risa.12503

Malterud, K., Siersma, V. D., & Guassora, A. D. (2016). Sample size in qualitative interview studies: Guided by information power. *Qualitative health research*, *26*(13), 1753–1760.

McFarlane, P., & Hills, M. (2013). Developing immunity to flight security risk: Prospective benefits from considering aviation security as a socio-technical eco-system. *Journal of Transportation Security*, *6*(3), 221–234. doi:10.1007/s12198-013-0113-3

McHendry, G. F. (2015). The re (*d*) active force of the transportation security administration. *Criticism*, *57*(2), 211–233. doi:10.13110/criticism.57.2.0211

Merriam, S. B. (2014). Qualitative Research: A guide to design and implementation. Hoboken, NJ: Wiley

Meuter, R. F. I., & Lacherez, P. F. (2016). When and why threats go undetected: Impacts of event rate and shift length on threat detection accuracy during airport baggage screening. *Human Factors: The Journal of Human Factors and Ergonomics Society*, *58*(2), 218–228. doi:10.1177/0018720815616306

Moustakas, C (1994). Phenomenological research methods. Thousand Oaks, CA: Sage Publications.

Muller, J. (2011). Terror, Security, and Money. *Balancing the Risks, Benefits and Cost of Homeland Security*. Retrieved from https://calhoun.nps.edu/bitstream/handle/10945/24979/109.pdf?sequence=1

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence-Based Nursing*, *18*(2), 34–35.

Olson, J. D., McAllister, C., Grinnell, L. D., Walters, K. G., & Appunn, F. (2016). Applying constant comparative method with multiple investigators and inter-coder reliability. *The Qualitative Report*, *21*(1), 26.

Palthe, J. (2014). Regulative, normative, and cognitive elements of organizations: Implications for managing change. *Management and Organizational Studies*, *1*(2), 59–66. doi:10.5430/mos. v1n2p59

Pasquariello, P. (2014). Prospect theory and market quality. *Journal of Economic Theory*, *149*, 276–310. doi: 10.1016/j.jet.2013.09.010

Paté-Cornell, E., & Cox, L. A. (2014). Improving risk management: From lame excuses to principled practice. *Risk Analysis*, *34*(7), 1228–1239. doi:10.1111/risa.12241

Peters, B. G. (2012). Governance as political theory. In civil Society and Governance in China (pp. 17-37). Basingstoke, United Kingdom: Palgrave Maemillan.

Pettersen, K. A., & Bjørnskau, T. (2015). Organizational contradictions between safety and security - perceived challenges and ways of integrating critical infrastructure protection in civil aviation. *Safety Science*, *71*, 167–177. doi: 10.1016/j.ssci.2014.04.018

Pinho, J. C. (*2017;2016;*). Institutional theory and global entrepreneurship: Exploring differences between factor- versus innovation-driven countries. *Journal of International Entrepreneurship,* 15(1), 56-84. Doi:10.1007/s10843-016-0193-9.

Poole, R., & Carafano, J. (n.d.). *Time to Rethink Airport Security*. Retrieved from http://www.heritage.org/research/reports/2006/07/time-to-rethink-airport-security.

Poole, R. W. (2015). Cost Effective Airport Security Policy. In S. Hakim, G. Albert, & Y. Shiftan (Eds.), *Securing transportation systems*., (pp. 205-231). Hoboken, NJ: John

Wiley and Sons, Inc. Retrived from. Retrieved from https://doi.org/10.1002/9781119078203.ch11

Prezelj, I. (2015). Relationship between security and human rights in counter-terrorism: A case of introducing body scanners in civil aviation. *International Studies. Interdisciplinary Political and Cultural Journal*, *17*(1), 145–158. doi:10.1515/ipcj-2015-0010

Price, J., & Forrest, J. S. (2016). Practical aviation security: Predicting and preventing future threats (Third ed.). Kidlington, Oxford, United Kingdom: Butterworth-Heinemann. In *Practical aviation security: Predicting and preventing future threats*.

Riedl, D., Heuer, A., & Strauss, B. (2015). Why the three-point rule failed to sufficiently reduce the number of draws in soccer: An application of prospect theory. *Journal of Sport & Exercise Psychology*, *37*(3), 316.

Robinson, O. C. (2014). Sampling in interview-based qualitative research: A theoretical and prac-tical guide. *Qualitative Research in Psychology*, *11*(1), 25–41.

Rohner, D., Thoenig, M., & Zilibotti, F. (2013). War Signals: A theory of trade, trust and con flict. *The review of Economics Studies*, *80*(3), 1114–1147.

Rudner, M. (2015). Intelligence-led air transport security: Pre-screening for watch-lists, no-fly lists to forestall terrorist threats. *International Journal of Intelligence and CounterIntelligence*, *28*(1), 38–63. doi:10.1080/08850607.2014.962352

Sakano, R., Obeng, K., & Fuller, K. (2016). Airport security and screening satisfaction: A case study of US. *Journal of Air Transport Management*, *55*, 129–138. doi:10.1016/ j. jairtraman.2016.05.007

Sandler, T. (2014). The analytical study of terrorism: Taking stock. *Journal of Peace Research*, *51*(2), 257–271. doi:10.1177/0022343313491277

Schmidt, A. V. (2016). Cyberterrorism: Combating the aviation industry's vulnerability to cyberattack. *Suffolk Transnational Law Review*, *39*(1), 169.

Scott, W. R. (2004). Institutional theory. *In Encyclopedia of Social Theory*, George Ritzer, ed. Thousand Oaks, CA: Sage Publications,Inc.

Scott, W. R. (2014). *Institutions and organizations: Ideas, interests and identities* (Fourth ed.). Thousand Oaks, CA: Sage Publications, Inc

Screening Partnership Program: (2012). Why is a Job-creating, Public-private Partnership Meeting Resistance at TSA, 112-68 (Subcommittee on Transport Security February 7 & 16*, 2012*).

Scurich, N., & John, R. S. (2014). Perceptions of randomized security schedules. *Risk Analysis*, *34*(4), 765–770. doi:10.1111/risa.12126

Shafieezadeh, A., Cha, E. J., & Ellingwood, B. R. (2015). A decision framework for managing risk to airports from terrorist attack: A decision framework for managing terrorism risk. *Risk Analysis*, *35*(2), 292–306. doi:10.1111/risa.12266

Shen, Y., Tobia, M. J., Sommer, T., & Obermayer, K. (1298–1328). *Neural Computation, 26*. (7). doi:10.1162/ NECO_a_00600

Skorupski, J., & Uchronski, P. (2015). A fuzzy reasoning system for evaluating the efficiency of cabin baggage screening at airports. *Transportation Research Part C: Emerging Technologies*, *54*, 157–175. doi: 10.1016/j.trc.2015.03.017

Stewart, M. G., & Mueller, J. (2013a). Aviation security, risk assessment, and risk aversion for public decisionmaking. *Journal of Policy Analysis and Management*, *32*(3), 615–633. doi:10.1002/pam.21704

Stewart, M. G., & Mueller, J. (2013b). Terrorism risks and Cost?Benefit analysis of aviation security. *Risk Analysis*, *33*(5), 893–908. doi:10.1111/j.1539-6924.2012. 01905.x

Stewart, M. G., & Mueller, J. (2015). Responsible policy analysis in aviation security with an evaluation of PreCheck. *Journal of Air Transport Management*, *48*, 13. doi:10.1016/ j.jairtraman.2015.06.007

Transport Canada. (n.d.). Canada's National Civil Aviation Security Program. Transport Canada.

Transportation Security Administration. (2016). TSA's 2017 budget: A commitment to security. Retrieved from https://www.tsa.gov/news/testimony/2016/03/01/hearing-fy17-budget-request-transportation-security-administration. In *TSA's 2017 budget: A commitment to security*.

Valkenburg, G., & van der Ploeg, I. (2015). Materialities between security and privacy: A constructivist account of airport security scanners. *Security Dialogue*, *46*(4), 326–344. doi:10.1177/0967010615577855

Vorobeychik, Y., & Letchford, J. (2015). Securing interdependent assets. *Autonomous Agents and Multi-Agent Systems*, *29*(2), 305–333. doi:10.1007/s10458-014-9258-0

Wallace, R. J., & Loffi, J. M. (2014). The unmitigated insider threat to aviation (*part 2*) : An analysis of countermeasures. *Journal of Transportation Security*, *7*(4), 307–331. doi:10.1007/s12198-014-0150-6

Welch, K. (2016). Middle eastern terrorist stereotypes and anti-terror policy support: The effect of perceived minority threat. *Race and Justice*, *6*(2), 117–145. doi:10.1177/2153368715590478

Wigginton, M., Jensen, C. J., Graves, M., & Vinson, J. (2014). What is the role of behavioral analysis in a multilayered approach to aviation security? Journal of Applied Security Research, 9 (*4*), 393-417. doi:10.1080/19361610.2014.942828

Wong, S., & Brooks, N. (2015). Evolving risk-based security: A review of current issues and emerging trends impacting security screening in the aviation industry. *Journal of Air Transport Management*, *48*, 60. doi: 10.1016/j.jairtraman.2015.06.013

Wray, R. E., Bachelor, B., Jones, R. M., & Newton, C. (n.d.). Bracketing human per-formance to support automation for workload reduction: A case study. In *International Conference on Augmented Cognition* (pp. 153–163). New York, NY: Springer.

Yadav, D. K., & Nikraz, H. (2014). Implications of evolving civil aviation safety regulations on the safety outcomes of air transport industry and airports. *Aviation*, *18*(2), 94–103. doi:10.3846/16487788.2014.926641

Yin, R. K (2013). *Case study research:* Design and methods. Thousand Oaks, CA: Sage publications.

Yin, R. K (2014). *Case study research*: Design and methods. (5th ed.). Thousand Oaks, CA, Sage publications.