PNNL-25689

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle Since 1965

The Threat Among Us

Insiders Intensify Aviation Terrorism

August 2016

KE Krull

U.S. DEPARTMENT OF
ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <http://www.ntis.gov/about/form.aspx>
Online ordering: http://www.ntis.gov

This document was printed on recycled paper.
(8/2010)

PNNL-25689

The Threat Among Us

KE Krull

August 2016

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99352

Abstract

Aviation terrorism is powerful and symbolic, and will likely remain a staple target for terrorists aiming to inflict chaos and cause mass casualties similar to the 9/11 attacks on the U.S. The majority of international and domestic aviation terrorist attacks involves outsiders, or people who do not have direct access to or affiliation with a target through employment. However, several significant attacks and plots against the industry involved malicious employees motivated by suicide or devotion to a terrorist organization. Malicious insiders' access and knowledge of aviation security, systems, networks, and infrastructure is valuable to terrorists, providing a different pathway for attacking the industry through the insider threat. Indicators and warnings of insider threats in these cases exist, providing insight into how security agencies, such as the Transportation Security Administration, can better predict and identify insider involvement. Understanding previous aviation insider threat events will likely aid in stimulating proactive security measures, rather than reactive responses. However, similar to traditional airport security measures, there are social, political, and economic challenges in protecting against the insider threat, including privacy concerns and cost-benefit analysis.

Acknowledgments

The author would like to sincerely thank several individuals for their contributions to this research, including mentor Chrissie Noonan for her guidance and support throughout this process, Carolyn Cramer for her operational support and insight, and Alex Stephan, Lead for the Special Programs and Scientific Studies Team at Pacific Northwest National Laboratory. The Pacific Northwest National Laboratory is operated by Battelle for the U.S. Department of Energy under Contract DE-AC06-76RL01839.

Acronyms and Abbreviations

AIT	advanced imaging technology
AQAP	al-Qaeda in the Arabian Peninsula
DHS	U.S. Department of Homeland Security
DOS	U.S. Department of State
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
GTD	Global Terrorism Database
ISIS	Islamic State in Iraq and Syria
IT	internet technology
MRS	metro rail systems
PFLP	Popular Front for the Liberation of Palestine
TSA	Transportation Security Administration
U.K.	United Kingdom
UPS	United Parcel Service
U.S.	United States
USD	United States dollar

Contents

Abstract iii
Acknowledgments iv
Acronyms and Abbreviations v
1.0 Introduction 1
2.0 Discussion 3
2.1 Defining Terrorism and the Insider Threat 3
2.2 The Driving Forces behind Terrorism and Insider Threats 4
2.2.1 How do they relate? 5
2.3 Targeting Aviation 6
2.4 Case Studies of Aviation Attacks 9
2.4.1 Dawson’s Field Hijackings 9
2.4.2 Lockerbie Bombing 9
2.4.3 FedEx Flight 705 10
2.4.4 9/11 Attacks 10
2.4.5 Underwear Bomber Plot 10
2.4.6 UPS Cargo Planes Ink Cartridge Plot 11
2.4.7 German Co-pilot Hijacking Suicide 11
2.4.8 Ataturk Airport Bombings 11
2.4.9 Malaysia: A Final Example 12
2.5 Analysis of Patterns and Trends 16
2.6 Insider Threat Indicators 19
2.7 Aviation vs. Other Mass Transit Security 20
2.7.1 U.S. Aviation Security 20
2.7.2 Global Aviation Security 23
2.7.3 Train and Bus Security 23
2.8 Challenges in Protecting Aviation and Mass Transit 24
2.9 Effective and Ineffective Security Measures 26
2.10 Looking Forward 27
2.10.1 Politically 27
2.10.2 Economically 28
2.10.3 Physically 28
2.10.4 Further Research: Cyber Capabilities, Terrorism, and the Insider Threat 28
3.0 Conclusion 30
4.0 References 31
Appendix A A.1
Additional Case Study Data A.1

Figures

Figure 1. Globally Recorded Aviation Terrorist Attacks from 1970-2015 6
Figure 2. Global Aviation Terrorist Attacks by Region from 1970-2015 7
Figure 3. Breakdown of the Global Aviation Finances 8
Figure 4. Timeline of Case Study Aviation Terrorist Attacks 1970-2016 13
Figure 5. Primary Method of Attack 1970-2015 17
Figure 6. Primary Weapon Type 1970-2015 17
Figure 7. Number of Aviation Attacks by Region 1970-2015 18
Figure 8. Aviation Security Measures in Relation to Terrorist Attacks 22
Figure 9. TSA Expenditures 2005-2014 25
Figure 10. TSA Layered Security 26

Tables

Table 1. Significant Aviation Terrorist Attacks 14
Table 2. Indicators of Insider Threats (Source: Greitzer et al. 2014)... 20

1.0 Introduction

A decade and a half after the 11 September 2001 terrorist attacks that involved four hijacked aircraft crashing into and destroying the World Trade Center Twin Towers and severely damaging the Pentagon, aviation remains a staple target for terrorists. Although fatal hijackings and attacks on aircraft occurred well before these attacks (GTD 2015), 9/11 sparked the international community into launching new aviation security, procedures, regulations, and operations. There are political, economic, and social implications that act as motives of terrorism. Some terrorists claim that acts of violence are the better alternative to other forms of political protesting and promotion. Some join terrorist groups for financial reasons, such as providing for their families. Other people join terrorist groups because they are otherwise outcasts and lack a place in society (Abrahms 2008).

The insider is rising as one of the key threats to the aviation industry in relation to terrorism. Motives for malicious and intentional insider activity can be political, economic, social, cultural, and personal. Malicious insiders seeking revenge, sabotage, or espionage, and intentional insiders seeking a self-benefiting profit are aware that their access to materials, systems, networks, and infrastructure is valuable to terrorists. They can provide terrorists with access to information about a company or significant building that would aid in an attack, such as the layout of an airport. Terrorists can also recruit insiders to act on their behalf or attempt to become the insider to carry out an attack by gaining authorized access to facilities, systems, and data.

There are several potential political, economic, and physical responses to improving security and combatting the insider threat challenge in terrorism aviation. They require international cooperation and an in-depth focus on insider threat awareness and training in the U.S. aviation industry. Understanding the indicators and warnings of previous aviation insider threat events will aid in stimulating proactive security measures, rather than reactive responses. Implementing these measures will likely aid in preventing future terrorist attacks on aviation involving insider threats. Many challenges in aviation security remain in existence, with issues ranging from low-level security employees to top management of security agencies.

2.0 Discussion

2.1 Defining Terrorism and the Insider Threat

Terrorism is a prevalent conflict that influences many nations internationally, making it difficult to establish an agreed upon definition of the concept. There are many definitions of terrorism, varying between different United States (U.S.) agencies, international actors, and academics. These differences are likely due to different objectives between departments. The Department of State (DOS) defines terrorism as, "premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence an audience" (DOS, in Gearson 2002). The Federal Bureau of Investigation (FBI) defines it as, "the use of serious violence against persons or property, or the threat to use such violence, to intimidate or coerce a government, the public, or any section of the public in order to promote political, social, or ideological objectives" (FBI, in Gearson 2002). The UK's Terrorism Act 2000 describes terrorism as, "the use or threat of serious violence against persons or serious damage to property, designed to influence the government or intimidate the public or a section of the public…for the purpose of advancing a political, religious, or ideological cause" (U.K. Terrorism Act 2000, in Gearson 2002).

Although most definitions include the concept of the use or threat of violence by non-state actors to reach a specific audience the lack of a cohesive, universal, and agreed upon definition can create discrepancies in data recording and analysis. The Global Terrorism Database (GTD) defines a terrorist attack as, "the threatened or actual use of illegal force and violence by a non-state actor to attain a political, economic, religious, or social goal through fear, coercion, or intimidation" (GTD 2016). The GTD is an open-source database including information on global terrorist events since 1970 and is operated by University of Maryland's Study of Terrorism and Responses to Terrorism (START) program.[1] The U.S. Department of Homeland Security (DHS) funds this program (START 2016). The majority of the aviation terrorist attacks analyzed in this report are from the GTD, making its definition of terrorism the primary for this report.

To classify incidents as terrorist attacks, they must be intentional, entail some level of violence or immediate threat of violence – against either people or property, – and the perpetrators must be sub-national actors. The actors must be aiming to attain a political, economic, religious, or social goal; however, the pursuit of profit alone with no goal of systematic economic change does not satisfy this criterion. There must be evidence of an intention to coerce, intimidate, or convey some other message to a larger audience than the immediate victims, and the action must be outside of the context of legitimate warfare activities permitted by international humanitarian law (GTD 2016).

Similar to that of terrorism, definitions of insider threats vary between private sector entities and the government, leading to disagreements regarding what constitutes an insider threat. However, one agreed upon notion is that the insider is an individual presently or previously authorized to access an organization's information system, data, or network. According to the U.S. government, "an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the U.S. through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities" (NCSC 2011).

[1] For details regarding definitions of GTD classification and criterion, refer to https://www.start.umd.edu/gtd/downloads/Codebook.pdf

Across the private sector, most organizations agree that the insider threat refers to, "harmful acts that trusted individuals might carry out; for example, something that causes harm to the organization, or an unauthorized act that benefits the individual" (Greitzer et al. 2014). Both definitions are applicable in the context of this report. Examples of serious abuse of privileges and crimes include espionage, insider trading, sabotage, terrorism, embezzlement, extortion, bribery, corruption, and intellectual property theft. Other incidents of insider threats that are largely disagreed upon include workplace violence, and in some cases, suicide. Although generally related to the cybersecurity of company networks and systems, the insider threat remains a physical security concern.

There are three types of insider threats: malicious, intentional, and unintentional. Malicious insiders intend to cause direct harm or damage to their place of employment with a motive of either personal gain or revenge. Intentional or non-malicious insiders act for self-benefiting purposes without malicious intent. They are considered voluntary rule breakers, possibly causing damage or security risks. Unintentional or accidental insiders are those who, through action or inaction without malicious intent, cause harm or substantially increase the probability of future serious harm to the organization's confidentiality or integrity. This includes negligent employees who are willing to ignore policy to increase convenience, and well-meaning employees who value completing work over following policy (Ford 2015).

2.2 The Driving Forces Behind Terrorism and Insider Threats

Among experts, two explanations for the cause of terrorism exist. The more supported strategic model asserts that, "terrorists are rational actors who attack civilians for political ends" (Abrahms 2008) that are opposed by established governments (Crenshaw 1998). This model assumes that terrorism is resorted to when the expected political return is greater than with alternative options (Abrahms 2008). However, there are several arguments against the strategic model, including notions that suggest that terrorists are not rational because they rarely attain their policy demands by attacking civilians. When their political motives weaken, terrorist organizations resist disbanding and often create their own relevant political rationale, changing their mission and objectives and contradicting the model's assumption that terrorists have consistent and stable political goals (Abrahms 2008).

Organization theory, which hypothesizes that people become terrorists to "develop strong affective ties with other terrorist members," and for "social solidarity, not for political return," is another approach to terrorism (Abrahms 2008). Those that become terrorists are often struggling economically, are socially alienated, and sometimes feel that they do not have a place in their communities. A majority of terrorist organizations are composed of unmarried young men lacking employment (Abrahms 2008).

The structure of a terrorist organization, such as Islamic State in Iraq and Syria (ISIS), provides many benefits, including monetary, security, and social support. Terrorist organizations promote unity under one or more objectives, giving meaning to the lives of their followers. Socially, terrorists benefit from relationships with other terrorists. A study of 173 global jihadists found that members from various groups joined, not for political or ideological motives, but to maintain or develop social relations (Sageman, in Abrahms 2008). A study on al-Qaeda, Fatah, Hamas, Hezbollah, Palestinian Islamic Jihad, and Turkish terrorists claims that the main reason for members joining the terrorist organization was having a friend or family member already in it (Abrahms 2008).

Despite differences in these viewpoints, terrorists act on behalf of their organization's mission either in the form of full-scale battles or suicide bombings at heavily populated areas, such as airports. In attempting to promote their cause, terrorist organizations inflict violence on civilians, infrastructure, and governments.

In comparison, there are several factors that contribute to insider threats, including human, social, political, cultural, organizational, and economical influences. Human level factors include personal events and stressors, such as a recent divorce or the death of a loved one. Social, political, and cultural elements are often displayed in the workplace, especially within the government. At the organizational level, influences can include poor workplace performance and the passing of a promotion to another employee. These contributing factors, in conjunction with capabilities (access), motive – such as revenge, self-benefit, espionage, and intellectual property theft – intent, and opportunity, create the ideal circumstances for malicious or intentional insiders to act. Elements that influence the threat from unintentional or accidental insiders include workplace negligence, failure to follow policy, and a lack of training and awareness for employees throughout different departments in a company.

2.2.1 How Do They Relate?

Malicious insiders seeking revenge, sabotage, or espionage, and intentional insiders seeking a self-benefiting profit are aware that their access to materials, systems, networks, and infrastructure is valuable to criminals. Potential buyers of intellectual property or one's expertise and access include state actors, non-state actors, transnational criminal organizations, and terrorists. Insiders can provide an indirect avenue for terrorists to carry out their objectives. Malicious insiders with various motives, such as revenge, sabotage, and espionage can sell intellectual property, like materials to make a nuclear weapon, to a terrorist organization. In this case, once in possession of the property, the terrorists can either use it to create a weapon, reverse engineer the technology, store or keep it, partner with others to prepare for its use, trade it, use it for bribery, or use it as a deterrent from governments.

Terrorists can also recruit insiders to act on their behalf, indicating a high level of sophistication due to the knowledge of the insider target that the terrorist would need-to-know. This is exemplified in known al-Qaeda in the Arabian Peninsula (AQAP) operative Anwar al- `Awalqi's recruitment campaign via email and social media (CTC 2011). In 2011, Yemen authorities arrested an American who worked at five nuclear power plants in Pennsylvania and was recruited for his skills and access (ABC News 2011).

Malicious and intentional insiders can also provide terrorists with access to information about a company or significant building, like the layout of an airport, which would aid in an attack. This information includes security locations, easily accessible points of entry, and vulnerabilities within screening and security systems. An example of this is when in 2011, Rajib Karim, an internet technology (IT) employee at British Airways, maintained communication with AQAP in an attempt to provide al- `Awalqi with information on aviation security procedures. He also offered to supply the terrorist organization with information that could be used to stage a suicide attack, although this was unsuccessful as he was denied a cabin crew position. Prior to his arrest, Karim also attempted to recruit fellow Muslims, including a baggage handler and a security employee, to stage an attack. A John F. Kennedy International Airport employee involved in plotting a terrorist attack targeting fuel lines below the airport was found guilty in 2007 (CTC 2011).

Exploiting unintentional insiders is also a potential means for a terrorist organization to meet its objectives. Although highly unlikely due to a lack of terrorists' cyber capabilities, hacking and spear-phishing are increasingly popular methods of gaining remote access (TrendMicro 2016). With a continual increase in technology in industry and government, the number of vulnerabilities in systems and networks grows. Terrorists can exploit accidental insiders by physical means, such as the threat of force or violence.

A terrorist may attempt to become the insider, rather than exploiting one, to carry out an attack by gaining authorized access to facilities, systems, and data. Karim's attempt to obtain a position as a cabin crew member in order carry out a suicide bombing while onboard a British Airways plane is an example of this. In 2010, Takuma Owuo-Hagood became a baggage handler at Delta Airlines with intentions of providing the Taliban with sensitive information (CTC 2011).

In each of these cases, the terrorist or insider had a clear motive and, when presented with the opportunity, used their capabilities to attempt to carry out their objectives. Insiders abuse their privileges for various reasons, providing the opportunity for terrorists to strengthen and promote their own agendas.

2.3 Targeting Aviation

The global aviation industry remains a staple target for terrorists for several reasons. Aviation terrorism is powerful and symbolic, it provides an international stage and extensive media exposure, the consequences of a successful attack are significant on airlines and the government, it contributes to political embarrassment and vulnerability, and it is effective (Baker 2015).

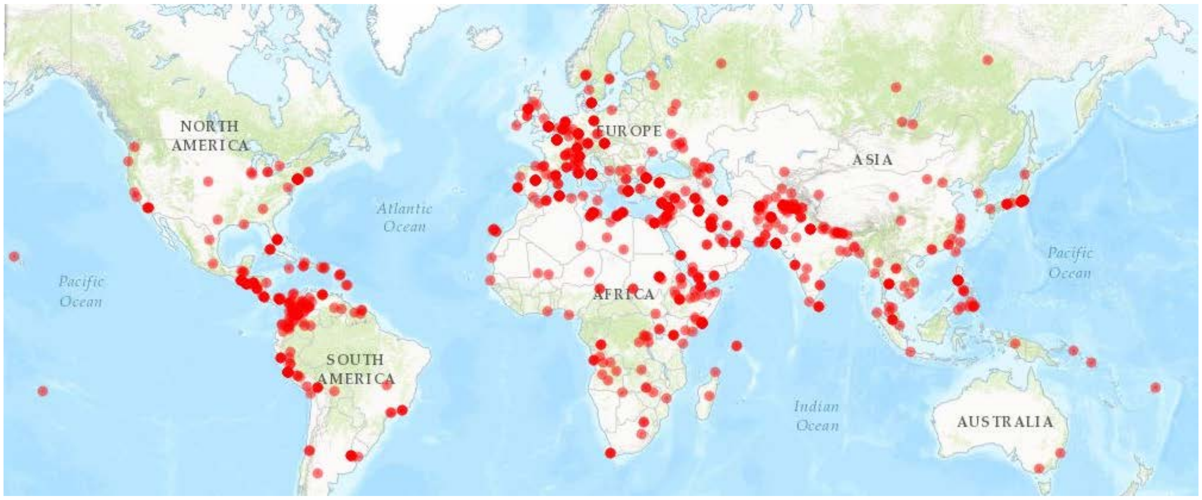

Figure 1. Globally Recorded Aviation Terrorist Attacks from 1970-2015
Source: GTD 2015

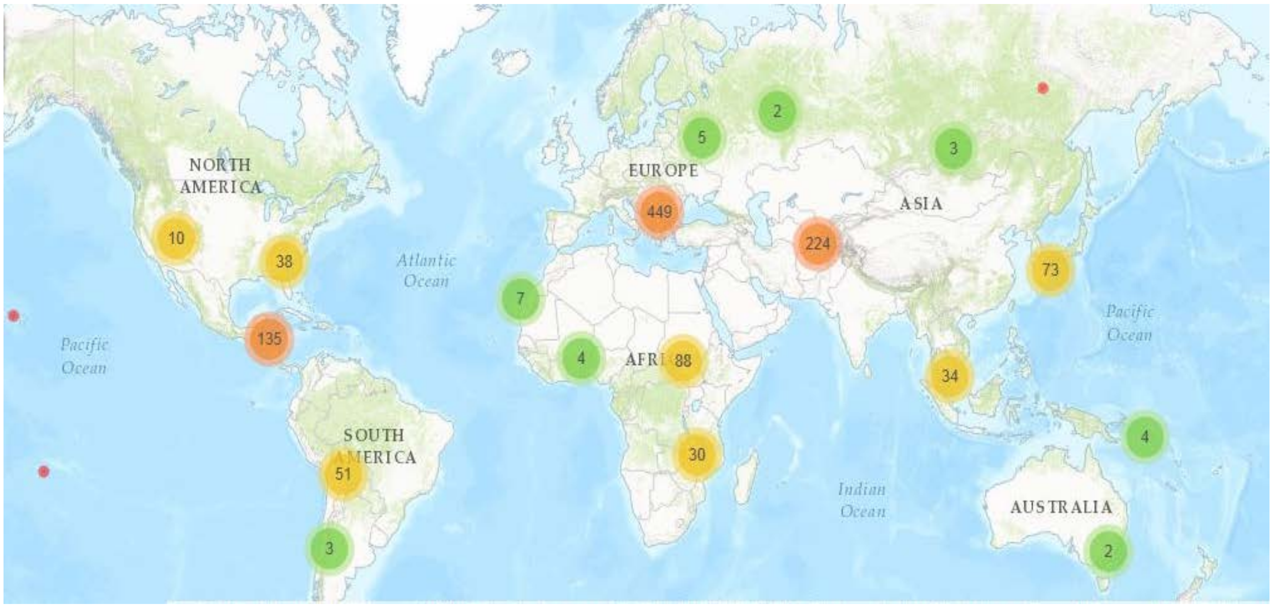

Figure 2. Global Aviation Terrorist Attacks by Region from 1970-2015
Source: GTD 2015

There are 1,363 GTD recorded terrorist attacks on airports and aircraft internationally from 1970-2015 (see Figures 1 and 2), as well as several unrecorded attacks in 2016.[1] Experts estimate that there will be approximately six billion passengers annually by 2030. The International Air Transport Association estimates that in 20 years, there will be a 4.1% annual growth rate in the number of global passengers, more than doubling to 7.3 billion from the current 3.3 billion (Gillen and Morrison 2015). The aviation industry is an effective target for terrorist objectives of inflicting violence on the maximum number of civilians and reaching a specific audience. Aside from causing mass casualties, attacks on airports and aircraft have significant economic, social, and political implications.

[1] Refer to the following link for a database of all GTD recorded aviation terrorist attacks from 1970-2015 https://www.start.umd.edu/gtd/search/Results.aspx?chart=target&casualties_type=&casualties_max=&target=6&count=100

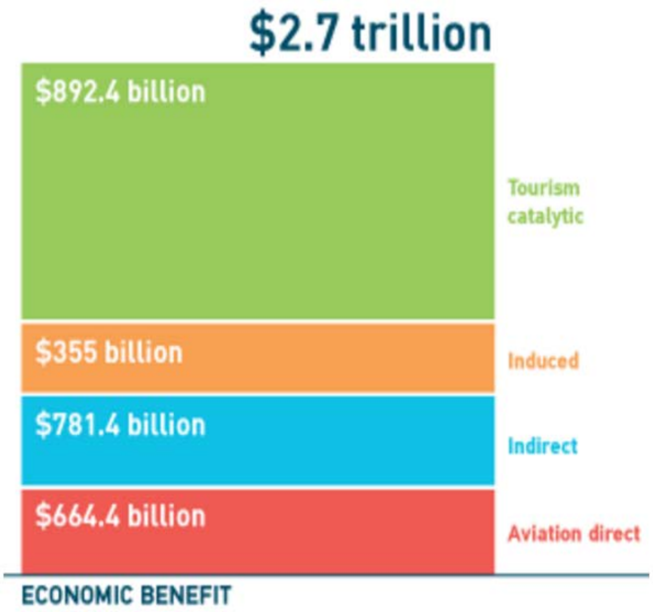

Figure 3. Breakdown of the Global Aviation Finances
Source: Aviation Benefits 2016

Aviation is a USD 2.7 trillion global industry that supports over 63 million jobs and is about 3.5 percent of the world's gross domestic product (Aviation Benefits 2016). In the U.S., aviation is a symbol of economic power, making it a continuously sought after target. Successful aviation terrorist attacks, such as those on property and businesses, are devastating to the economy. The 9/11 attacks cost the U.S. an estimated USD 243.6 billion. This includes the loss of four civilian aircraft (USD 385 million), the destruction of the World Trade Center (USD 3-4.5 billion), damage to the Pentagon (up to USD 1 billion), cleanup costs (USD 1.3 billion), property damage (USD 31.8-34.8 billion), federal emergency funds (USD 40 billion), job losses (USD 17 billion), loss of air traffic revenue (USD 10 billion), losses to the city (USD 95 billion),and losses to the insurance industry (USD 40 billion). The fall of global markets cost is incalculable, however, experts estimate that price would approach USD 2 trillion (IAGS 2004). Terrorists know that there are significant financial burdens in innovating new security measures in response to attacks, affecting the DHS budget (see Section 2.10.2 of this report).

The fear of flying instilled in passengers during the aftermath of successful attacks leads to airlines' decrease in customers, specifically tourists, which account for USD 892.4 billion (33 percent) of the industry's annual financials(see Figure 3). After 9/11, airlines experienced a total loss of USD 10 billion in air traffic revenue (IAGS 2004). Terrorists consider unsuccessful attacks, such as the Shoe Bomber bombing attempt, victories. This is likely due to the media and governmental attention that they draw, the economic consequences of updating security, and the assumption that the terrorists found vulnerability and defeated security.

Social implications of aviation terrorism exist. This includes instilling fear into the public, as well as the extensive media coverage drawn to the situation. One of terrorism's objectives is to reach a specific audience, and with international agencies and leaders focusing on the security and vulnerabilities of plots, terrorists achieve this goal. Political implications include embarrassment, as well as public disapproval. These attacks often evade security in some way, and therefore, new policy and security requirements are implemented after significant attacks on airplanes and airports that exploit weaknesses in security.

2.4 Case Studies of Aviation Attacks

Out of the 1,363 recorded aviation terrorist attacks in the GTD, along with other cases not yet recorded, there are several distinct attacks (GTD 2015). The distinctions include type of attack, weapons used, perpetrators, security failures, number of deaths, and indicators and warnings of the attacks or of insider threat involvement. The most significant and impactful of these attacks include, but are not limited to, the Dawson's Field Hijackings, the Lockerbie bombing, the 9/11 attacks, the Underwear Bomber plot, the United Parcel Service (UPS) Cargo Planes Ink Cartridge plot, the German co-pilot hijacking suicide, and the Ataturk Airport Bombings (see Table 1 and Figure 4). These attacks and plots heavily impacted aviation security and provide insight into the threat of insiders in aviation.

2.4.1 Dawson's Field Hijackings

On 6 September 1970, members of the Popular Front for the Liberation of Palestine (PFLP) hijacked four civilian aircraft departing to New York City from multiple airports in Europe. The hijackers took their total of 310 hostages, crew and passengers included, to an abandoned airport in a Jordanian desert. The PFLP demanded the release of captured PFLP militants held in the U.K., Switzerland, and Germany. Negotiations intensified between the U.S. and Israel, likely due to ongoing Cold War tensions. The U.S. and the Soviet Union were experiencing political fragility, and with the Soviet Union's support of almost all Arab Nations at the time, the U.S. struggled to bring Israel to aid in the conflict. After nearly six days of negotiations, extended deadlines, and the bombing of all four planes, the PFLP freed all 310 hostages and the Western nations returned the captured PFLP fighters (BBC 2005).

There were several indicators and warnings of the hijackings. The unsuccessful hijackers of the first plane bought their tickets in advance but picked them up at the last minute. Their four passports were sequential and the pilot and crew observed suspicious behavior among a pair that were sitting together in first class. The Palestinian pair were removed from the flight, however, their Western-appearing partners remained aboard – they later attempted to hijack the plane, but were unsuccessful, resulting in the death of one hijacker (PBS 2009). Additionally, the Palestinians removed from the original flight were immediately allowed to purchase new tickets for a different flight, which they successfully hijacked. Security failures of this incident include insufficient cockpit security, poor passenger and carry-on luggage screenings, as well as communication failures between airports and airlines. The next hijacking in the attack was several hours after the crew notified the authorities of the first attempt (PBS 2009).

2.4.2 Lockerbie Bombing

On 21 December 1988, approximately 38 minutes after takeoff from London, Pan Am Flight 103 exploded 31,000 feet over Lockerbie, Scotland. All 250 people on board the New York-bound plane and 11 people on the ground died. U.S. and British officials found fragments of a circuit board and a timer, indicating that it was a bombing, not a mechanical failure. The perpetrators are unknown. However a Scottish court found Libyan man, Adbel Basser Ali –al-Megrahi, guilty. Khalifa Fhimah was acquitted (CNN 2015).

Indicators and warnings of this attack include threats by the Libyan government in response to a series of bombing air strikes in Libya executed by the U.S. after the Libyan bombing of a nightclub in West Berlin frequented by U.S. military members. There are suspicions that former Libyan Prime Minister Gaddafi was involved in ordering the attack. There are also indicators of malicious insider threat involvement. Al-Megrahi was the Libyan intelligence aviation security chief and was seen bringing a suitcase very similar to the one found holding the explosive device to the Malta airport where the flight departed from. Fhimah was also the former Libyan Arab Airlines station manager at the Malta airport, indicating that he likely abused his access and privileges and aided al-Megrahi. The security failure in this case was poor checked baggage screening, specifically for employees (CNN 2015).

2.4.3 FedEx Flight 705

On 7 April 1994, a lone wolf named Auburn Calloway attempted to hijack a FedEx cargo plane bound for Memphis. The crew members were severely injured by a spear gun and a hammer that Calloway brought on board with him hidden in a guitar case. There were no fatalities (Newswire 2015).

Although there were no direct indicators or warnings of this aviation attack, there were several indicators that pointed to Calloway as a threat. He was an employee for FedEx, making him a malicious insider. Calloway was going through a recent divorce. His career was failing and he was about to be fired, driving his fear for his children's future and economic security. Additionally, Calloway's crew was grounded from flying for security purposes the day before the attack; however, he found a way to get onboard a plane anyway. The attempted hijacking was planned to end in a suicide crash that would appear as an accident. This would allow Calloway's children to collect his life insurance money (Newswire 2015). Security failures in this situation include poor employee screening and luggage screening, as well as failure on the part of the employer (Newswire 2015).

2.4.4 9/11 Attacks

On 11 September 2001, 19 al-Qaeda terrorists hijacked four commercial passenger jet airliners, crashing two into the Twin Towers at the World Trade Center in New York City and another into the Pentagon in Virginia. The fourth plane never reached its intended target, crashing in Pennsylvania, likely due to passengers and crew overpowering the hijackers. Including those on board the flights and in the targeted buildings, 2,997 people were killed. This is the largest loss of life due to a terrorist attack on U.S. soil. The 9/11 attacks are symbolic because the Twin Towers were widely considered symbols of America's power and influence and the Pentagon is the U.S. Department of Defense's headquarters. The U.S. and global markets experienced an incalculable amount of damage (BBC 2016). These are the most fatal aircraft attacks to date, and the single most fatal terrorist attack in the U.S. (BBC 2016).

Numerous indicators and warnings of these attacks existed. The FBI had evidence of al-Qaeda surveillance of federal buildings in New York City and Washington D.C. Al-Qaeda was heavily recruiting male Muslim-American youth in the U.S. Osama Bin Laden promised to follow the 1994 World Trade Center bombing as an example and to attack the U.S. Al-Qaeda recruits were taking flying lessons, but never learned how to land (The National Security Archive 2001). Along with a major intelligence failure, security failed as well. The cockpits in all four planes were unguarded and unlocked, allowing for easy access and leaving the pilots vulnerable. Additionally, aside from the plane that crashed in Pennsylvania, the passengers did very little to take back the aircraft (BBC 2016 and the National Commission on Terrorist Attacks Upon the United States 2004).

2.4.5 Underwear Bomber Plot

On 25 December 2009, al-Qaeda member Umar Farouk Abdulmutallab boarded a plane in the Netherlands bound for Detroit. He attempted to detonate plastic explosives hidden in his underwear while on the Northwest Airlines flight. After remaining in the aircraft's restroom for over 20 minutes, Abdulmutallab returned to his seat. Moments later, he attempted to detonate the bomb, however, the explosives failed, starting a fire in Abdulmutallab's underwear. A passenger extinguished the fire and the plane made an emergency landing. No casualties occurred (ABC News2012).

Indicators and warnings of this attack include passenger accounts of a wealthy looking man at the gate with the terrorist insisting the Abdulmutallab board without a valid passport. He also only had carry-on luggage for a two-week international trip. MI5, the U.K.'s security service, collected intelligence that linked him to extremists (ABC News 2012). The security failures in this case include poor passenger screening and a lack of information sharing among international security agencies.

2.4.6 UPS Cargo Planes Ink Cartridge Plot

On 29 October 2010, British authorities foiled a plot to bomb a UPS cargo plane over the U.S. AQAP claimed responsibility for the explosives hidden in ink cartridges onboard aircraft departing from the U.K. and Dubai. A mobile device connected to the detonator was set to go off at 8:30 a.m. Eastern Standard time. The ink cartridges were addressed to a synagogue in Chicago, although it is unknown if that was the target (The Guardian 2010).

Saudi intelligence claimed that there would be an aircraft attack relatively soon on a plane inbound to the U.S. (The Guardian 2010). The flaws in this instance were technological. The bombs were more sophisticated than what the explosive detection technology could detect at the time. The bomb in Dubai traveled on two passenger planes without being detected (The Guardian 2010).

2.4.7 German Co-pilot Hijacking Suicide

On 24 March 2015, a Germanwings Airlines co-pilot, Andres Lubitz locked the pilot out of the cockpit when he left for the restroom and hijacked the plane mid-flight. He crashed the aircraft into the French Alps, killing all 150 passengers and crew. He acted as a lone wolf, with no terrorist organization connections (CNN 2015).

There are no direct indicators or warnings of this specific attack; however, there are indicators of Lubitz being an insider threat. Although he previously mentioned severe depression incidents and suicidal tendencies to his boss and being deemed "unfit to work" by a doctor, Lubitz failed to report this to his employer (CNN 2015). Security failures in this case derive from a security measure set in place in response to 9/11: locked cockpits. Additionally, the employer failed to perform a thorough background check on a potential pilot with a history of mental illness.

2.4.8 Ataturk Airport Bombings

On 28 June 2016, two ISIS terrorists entered the Ataturk Airport in Istanbul shooting guns and eventually detonating suicide vests. Another terrorist mirrored those actions in a nearby parking lot. The terrorists attacked large crowds in unsecured portions of the airport, killing 42 and injuring 239. Although not directly claimed by ISIS, the attack has many hallmarks of those in Brussels and Paris due to the target and method, specifically the weapons and explosions (CNN 2016).

The indicators for this attack were the increasing number of terrorist cells linked to ISIS in Turkey, as well as ISIS threats against the country (CNN 2016). The major security failure in this attack was the mass crowding in areas before passing through security, creating a heavily populated target for perpetrators.

2.4.9 Malaysia: A Final Example

In June 2016, Malaysia’s Immigration Department fired 15 of its officials after uncovering a security breach that likely began in 2010. As many as 100 people were involved in allowing certain passengers to travel unchecked through the country’s main international airport (Intel News 2016). Malaysian officials are classifying this breach as sabotage due to the abuse of privileges on a computer system that checks travelers’ passports against databases that include lists of lost and stolen passports. With the system going offline, passport control officers have to manually screen passengers, likely permitting countless individuals with stolen and forged passports through security undetected (Intel News 2016).

This corruption, mismanagement, and failure to follow security standards compromised the Immigration Department and left the nation vulnerable to terrorists that may have easily have entered the country during a six year period. Airport and global aviation security were left exposed to potential terrorists due to the negligence and actions of the insiders. Officials believe that the malicious insiders were working online and receiving instructions from a criminal group overseas. The criminals were granted access to the system and could “move the cursor without someone physically operating it” (Time 2016). This finding reveals that insider threats are growing and that passport security is becoming increasingly vulnerable. This is another tactic that terrorists can use to exploit and inflict violence on aviation.

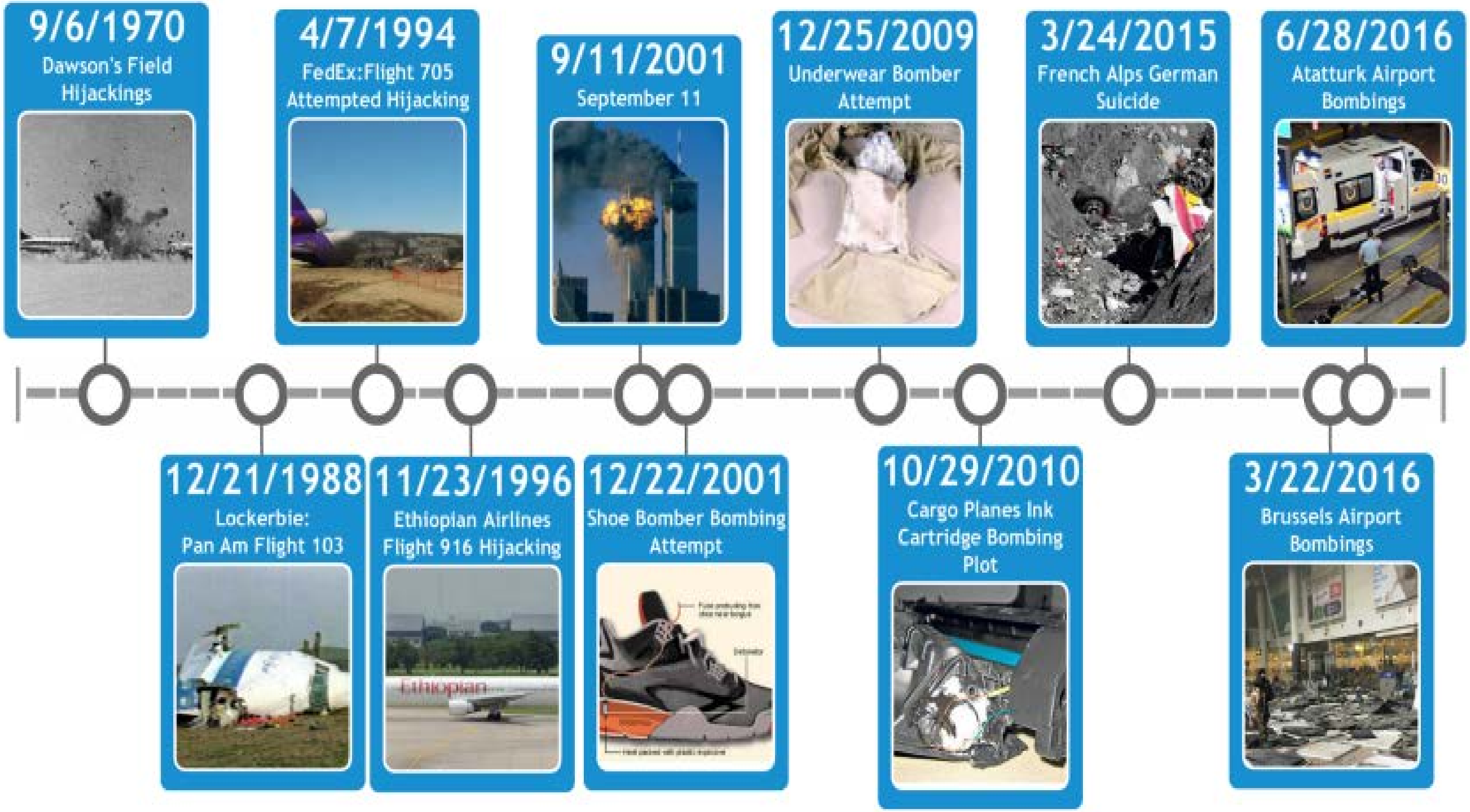
9/6/1970
Dawson's Field Hijackings
4/7/1994
FedEx:Flight 705 Attempted Hijacking
9/11/2001
September 11
12/25/2009
Underwear Bomber Attempt
3/24/2015
French Alps German Suicide
6/28/2016
Atatturk Airport Bombings
12/21/1988
Lockerbie: Pan Am Flight 103
11/23/1996
Ethiopian Airlines Flight 916 Hijacking
12/22/2001
Shoe Bomber Bombing Attempt
10/29/2010
Cargo Planes Ink Cartridge Bombing Plot
3/22/2016
Brussels Airport Bombings

Figure 4. Timeline of Case Study Aviation Terrorist Attacks 1970-2016
Sources: Cited in Text

Table 1. Significant Aviation Terrorist Attacks

Date	Attack	Location	Classification	Perpetrators (Affiliation)	Deaths	Indicators and Warnings	Indicators and Warnings of Insider Threat
6-Sep-70	Dawson's Field	European Airports-Zarqa	Hijackings	PFLP	1	Suspicious passengers bought tickets in advanced, picked them up at the last minute; passports in sequence, Palestinians removed from flight on 9/6 were able to purchase new tickets	N/A
21-Dec-88	Pan Am Flight 103	Lockerbie	Bombing/Explosion	Unknown; Libyan Abdel Basser Ali al-Megrahi convicted; Libyan Lamen Khalifa Fhimah acquitted; Libyan Prime Minister	270	Likely a response to bombing air strikes against Libya after the Libyan bombing of a nightclub in West Berlin frequented by U.S. military members	Malicious Insider: al-Megrahi was the Libyan intelligence aviation security chief; Fhima was the former Libyan Arab Airlines station manager in Malta
7-Apr-94	FedEx Flight 705	Memphis, TN	Armed Assault	Lone wolf: Auburn Calloway	0	N/A	Malicious Insider: Somewhat recent divorce; failing career, about to be fired; high level of concern for children's' future; crew grounded but flew anyway
23-Nov-96	Ethiopian Airlines Flight 916	Addis Ababa	Hostage taking	Lone wolves seeking asylum in Australia	123	N/A	N/A
11-Sep-01	American Airlines Flights 11 and 77; United Airlines Flights 175 and 93	New York City, NY; Arlington, VA; Shanksville, PA	Hijackings	Al-Qaeda	2,997	FBI evidence of al-Qaeda surveillance of federal buildings in New York City and D.C.; recruitment activity; Bin Laden promises to follow the 1994 World Trade Center bombing; recruits began taking flying lessons, never learned how to land	N/A

Date	Attack	Location	Classification	Perpetrators (Affiliation)	Deaths	Indicators and Warnings	Indicators and Warnings of Insider Threat
22-Dec-01	Shoe Bomber American Airlines Flight 63	Paris-Miami	Failed Bombing/Explosion	Al-Qaeda: Richard Colvin Reid	0	Became radicalized during prison sentence; traveled to Pakistan and Afghanistan; physical appearance raised suspicions; did not answer all questions, no checked luggage for overseas flights	N/A
25-Dec-09	Underwear Bomber	Detroit	Failed Bombing/Explosion	Al-Qaeda: Umar Farouk Abdulmutallab	0	Passenger accounts of a wealthy looking man insisting that Abdulmutallab board even without a passport; only carry-on luggage for a 2 week trip internationally; MI5 intel he linked to extremists	N/A
29-Oct-10	UPS Cargo Planes Ink Cartridge Bombing Plot	Sana'a	Bombing/Explosion	AQAP	0	Saudi intel that an attack with an aircraft would occur soon	N/A
24-Mar-15	German Suicide	French Alps	Hijacking	Lone wolf: Andreas Lubitz	150	N/A	Malicious Insider: Treated for suicidal tendencies; declared unfit to work by a doctor, kept from employer; previously informed employer of depression
22-Mar-16	Brussels Airport Bombings	Brussels	Bombing/Explosion, Armed Assault	ISIS	32	N/A	N/A
28-Jun-16	Ataturk Airport	Istanbul	Bombing/Explosion, Armed Assault	ISIS	42	ISIS warnings of attacks in Turkey and a large number of terrorist cells linked to ISIS	N/A

The data in this chart is from the GTD. References for the indicators and warnings columns are listed in Section 4 of this report.

2.5 Analysis of Patterns and Trends

Within the previously discussed attacks, there are similarities and differences in the characteristics of the events; these are within the offenders, victims, attack type, weapons used, and airlines (see Appendix A for a more detailed table of characteristics). Patterns begin to form and become trends over time. There are two types of offenders: terrorist members acting on behalf of or in response to an established terrorist organization and lone wolves. In six of the attacks discussed above, the offenders were radicalized extremists. In the case of the Dawson's Field Hijackings, the offenders were part of a military-like group attempting to promote the Palestinian cause. The 9/11 terrorists carried out the attack in groups of al-Qaeda members. The attempted shoe bombing failure in 2001, three months after 9/11, involved a person who proclaimed allegiance to al-Qaeda. Abdulmutallab, although acting alone on the day of the attempted underwear bombing, reported to and worked with al-Qaeda operatives and a well-known bomb maker. The recent attacks in the Brussels and Istanbul airports are attributed to ISIS. Terrorists attack aviation in small groups or individually, likely due to high levels of security. It is likely more efficient and effective to pass smaller numbers through security.

Although civilians are the main target for aviation, the potential consequences of a cargo plane attack are beneficial to terrorists. If the UPS ink cartridge attacks were successful, they would have likely resulted in significant economic loss, casualties on the ground resulting from falling aircraft debris, and international media coverage, giving al-Qaeda a large and international audience.

In contrast to offenders consisting of members of terrorist organizations, there is a trend of lone wolves taking advantage of aviation. Although likely tied to political and military motives of the Libyan government, only one suspect, lacking ties with terrorist organizations, was sentenced. As an insider himself, it is likely that Megrahi had assistance from Fhimah, an employee at the Malta airport. A lone wolf malicious insider attempted a hijacking suicide of a FedEx cargo plane.

It is difficult to distinguish specific trends within the victims of these attacks due to international flights. Often, terrorists aim to attack Westerners. This is displayed in the Dawson's Field hijacking and even more so in the 9/11 attacks. Americans will continue to be targets of interest to groups such as al-Qaeda. However, with the rise of ISIS and in light of the Brussels and Istanbul airport attacks in 2015 and 2016, it is evident that the victim type is becoming less of a trend.

There are several attack classifications used by the GTD, including, but not limited to: hijackings, bombings and explosions, armed assaults, and hostage taking. In the beginning of aviation terrorism, hijackings were the preferred modus operandi. However, patterns in attacks are revealing that this evolved into a trend of bombings and explosions as the primary method (see Figure 5). Therefore, the most common weapons used are explosives/bombs/dynamite, followed by firearms, and vehicles, meaning the aircraft itself. Using the aircraft as the weapon is more cost-effective to terrorist organizations than creating explosives (see Figure 6).

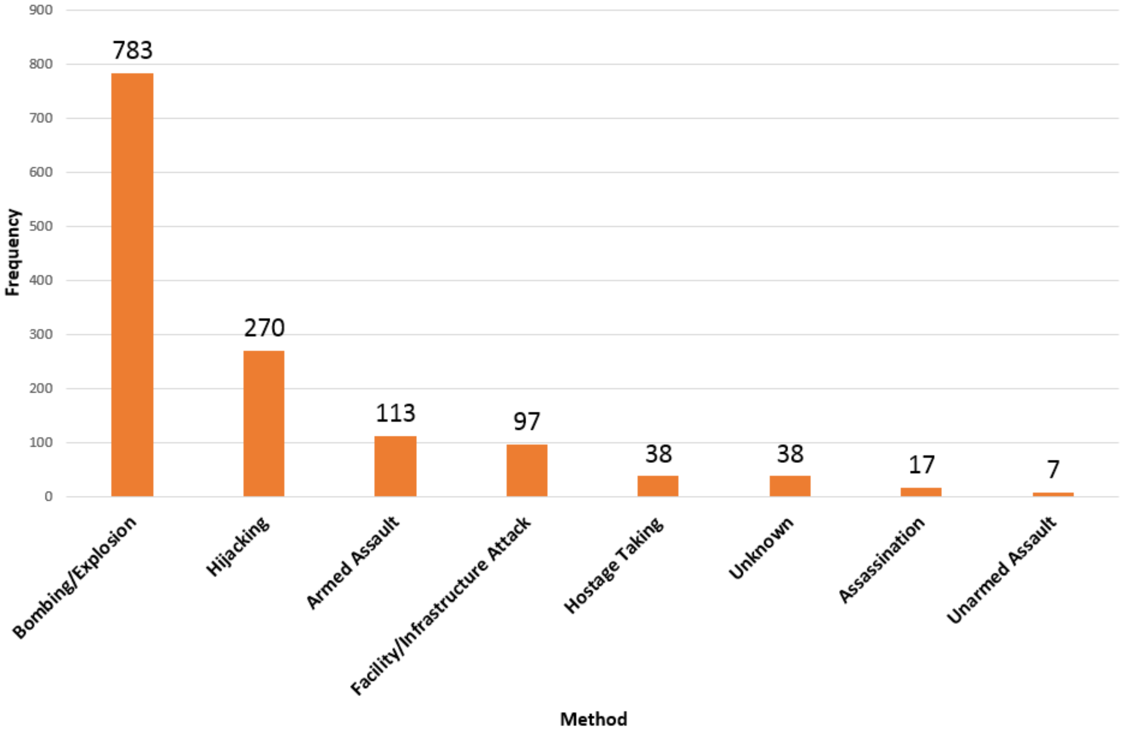

Figure 5. Primary Method of Attack 1970-2015
Source: GTD 2015

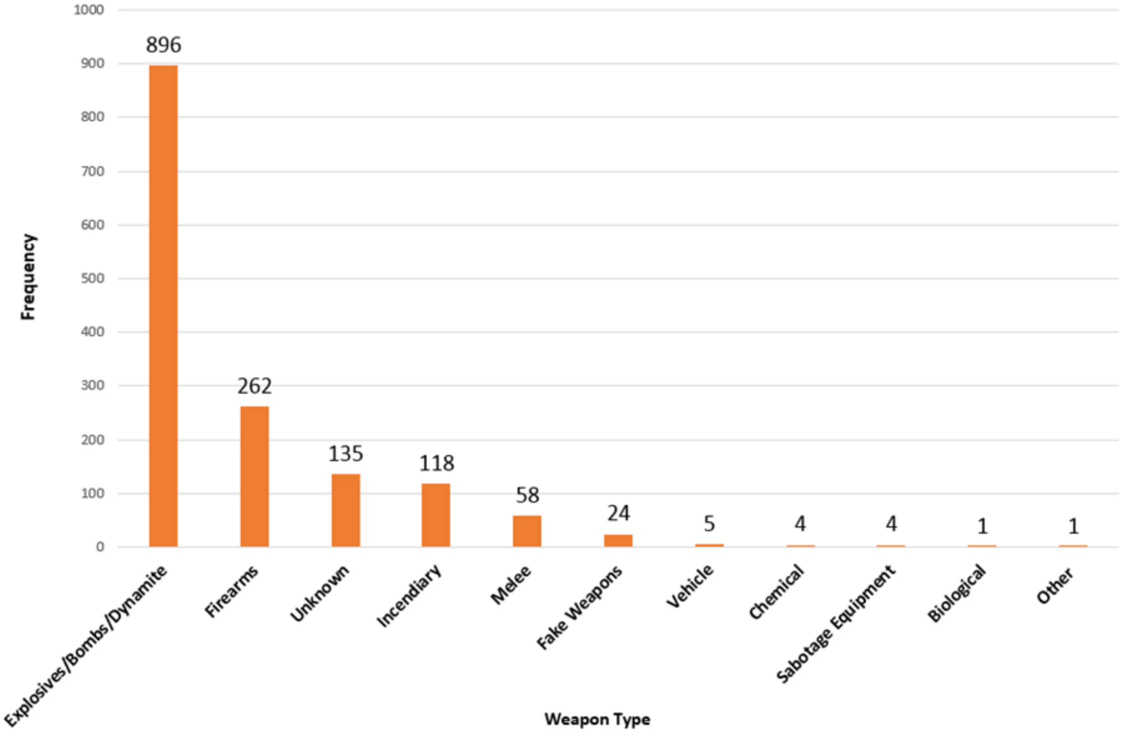

Figure 6. Primary Weapon Type 1970-2015
Source: GTD 2015

A pattern within airlines is the symbolism of words such as "United" in United Airlines and "American" in American Airlines, two U.S. airlines used in multiple attacks, specifically 9/11 (BBC 2016). There are also more attempts to attack international flights due to several global security issues (see Section 2.7.2 of this report).

Terrorists target the largest and busiest airports, such as John F. Kennedy International Airport because it records the most international departures in the U.S. The Istanbul Airport attack was successful largely due to the number of people inside the unsecure areas and because it is the eleventh busiest airport in the world. It is the third busiest in Europe, transiting 62 million passengers in 2015. Targeting larger airports increases the likelihood of mass casualties and sends a strong message. However, the majority of aviation terrorist attacks recorded by the GTD from 1970 through 2015 occurred in the Middle East (see Figure 7).

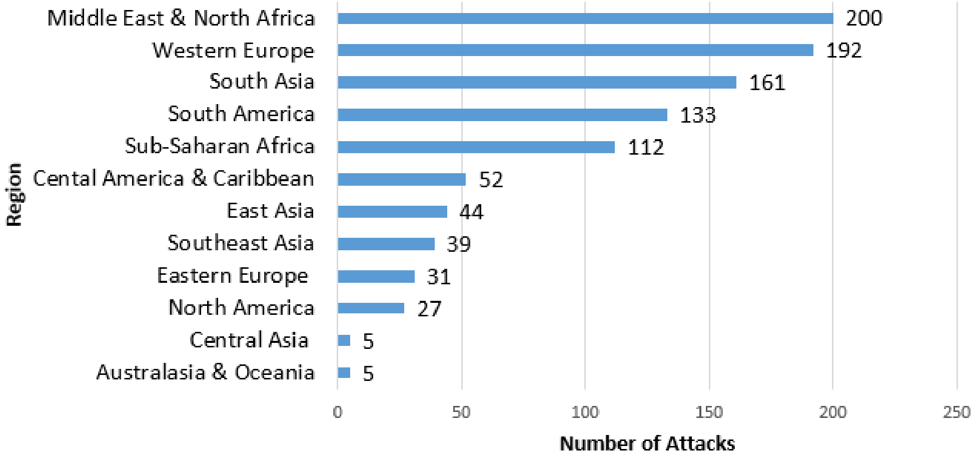

Figure 7. Number of Aviation Attacks by Region 1970-2015
Source: GTD 2015

One of the major trends in security failures derives from the many successes in smuggling bombs and explosives onboard aircraft. This is both a human and technological issue. A relatively new pattern in airport attacks is targeting the dense crowds in unsecured areas, such as the main entrance and baggage claims. ISIS used this tactic in Brussels and Istanbul. Poor passenger and employee screening also heavily contribute to these attacks. Additionally, airports, airlines, and federal agencies implement security measures in a reactive manner – usually in response to an attack that exploited a security vulnerability – rather than proactively to protect against the threat as a whole (see Section 2.10 of this report).

A trend in the insider threats involved in these attacks is that they either have ties to terrorist organizations through recruitment, self-allegiance, or they act as lone wolves. Those with ties to terrorists, such as the previously discussed plots by Owuo-Hagood and Karim, tend to provide information to the organizations rather than permitting physical access. This aids terrorist plots and mitigates the need for surveillance by an outsider, as seen in the JKF Airport plot. The lone wolves typically use aviation as an outlet for suicide, although it is unknown why they take other lives with them, as displayed in the Germanwings co-pilot suicide. In the context of aviation, insider threats are people that physically attempt to carry out malicious intent, as opposed to insiders looking for revenge or sabotage through cyber means. Insider threats range from low-level employees, such as baggage handlers and IT workers, to high level managers and officers. This indicates that there is a lack of proper security measures regarding access controls and privileges granted based on need-to-know data.

2.6 Insider Threat Indicators

Insider threats are continuing to increase in almost all areas of the public and private sectors and is "manifested when human behavior departs from compliance with established policies, regardless of whether it results from malice or a disregard for security policies" (Greitzer et al. 2007). One of the reasons for the growing number of opportunities to obtain revenge, sabotage, and financial benefits is due to an increase in cyber-dependent systems and technology (CERT 2016). There are two steps in detecting insiders: determining who has the capability to launch an attack or (Bishop et al. 2010), in the context of aviation, who has access to vulnerable sections of airports, as well as access to security protocol information. Access to these systems equals an opportunity for an attack. The second method is to determine which of those with the capability to attack are likely to do so (Bishop et al. 2010).

Several indictors of insider threats known by human resource staff to raise high levels of concern include but are not limited to performance, stress, self-centeredness, and personal issues (see Table 2). In the case of calculating psychosocial risk of insider threats, these indicators carry different weights (Greitzer et al. 2010). These indicators are evident within previously discussed attacks. Auburn Calloway, a lone wolf, attempted to hijack a FedEx cargo plane to commit suicide. He previously showed signs of poor performance, was about to lose his job, experienced severe stress over the personal issues of fear for his children's future and a recent divorce. The Germanwings suicide hijacker, Andreas Lubitz, previously received treatment for severe episodes of depression and a doctor declared him "unfit" to work. Rajib Karim, an IT employee at British Airways, offered to supply al-Qaeda with information that could be used to stage a suicide attack. He was previously overlooked for a job promotion as a cabin crew member.

These psychosocial indicators are beneficial to employers in detecting insider threats. Computer and technology aid in tracking and detecting insider activity on networks, however computers cannot determine human intent, which is more evident in the cases discussed above (Bishop et al. 2010). In the case of the Malaysian Immigration Department passport breach, there are indicators specific to computer network insider activity that might have assissted officials in detecting the threat earlier. This includes the system crashing frequently and the visibility of the cursor moving on the screen while no one was physically touching it. Proper network detection and scans would likely detect these indicators sooner. Understanding malicious insiders' intent and behavior will assist the security process by allowing officers and employees to better recognize insider activity.

Table 2. Indicators of Insider Threats (Source: Greitzer et al. 2014)

Indicator	Description
Disgruntlement	Employee observed to be dissatisfied in current position; chronic indications of discontent, such as strong negative feelings about being passed over for a promotion or being underpaid, undervalued; may have a poor fit with current job.
Not Accepting Feedback	The employee is observed to have a difficult time accepting criticism, tends to take criticism personally, or becomes defensive when message is delivered. Employee has been observed being unwilling to acknowledge errors or admitting to mistakes; may attempt to cover up errors through lying or deceit.
Anger Management Issues	The employee often allows anger to get pent up inside; employee has trouble managing lingering feelings of anger or rage; holds strong grudges.
Disengagement	The employee keeps to self, is detached, withdrawn, and tends not to interact with individuals or groups; avoids meetings.
Disregard for Authority	The employee disregards rules, authority or policies. Employee feels above the rules or that they only apply to others.
Performance	The employee has received a corrective action (below expectation performance review, verbal warning, written reprimand, suspension, termination) based on poor performance.
Stress	The employee appears to be under physical, mental, or emotional strain or tension that he/she has difficulty handling.
Confrontational Behavior	Employee exhibits argumentative or aggressive behavior or is involved in bullying or intimidation.
Personal Issues	Employee has difficulty keeping personal issues separate from work, these issues interfere with work.
Self-Centeredness	The employee disregards needs or wishes of others, concerned primarily with own interests and welfare.
Lack of Dependability	Employee is unable to keep commitments /promises; unworthy of trust.
Absenteeism	Employee has exhibited chronic unexplained absenteeism.

2.7 Aviation Versus Other Mass Transit Security

2.7.1 U.S. Aviation Security

Compared to other forms of mass transit, the aviation industry has the most structured security aimed at preventing terrorist attacks on its infrastructure. In efforts to prevent another 9/11-like attack on the U.S., the Transportation Security Administration (TSA) and the Federal Aviation Administration (FAA) work in conjunction with airlines and airport law enforcement officers to implement and enforce security measures and requirements.

In response to the 9/11 attacks, the 2001 U.S. Aviation and Transportation Security Act created the TSA, which is responsible for protecting the nation’s transportation systems to “ensure freedom of movement for people and commerce” (TSA 2016). This includes screening passengers in airports, verifying passports and identities through facial recognition, and working with local airport law enforcement. The FAA is the national aviation authority with powers to regulate all aspects of U.S. civil aviation, including setting guidelines and policy requirements. The U.S. aviation industry is part of the Public Transportation Information Sharing and Analysis Center, an entity that provides a 24/7 security operating capability that establishes the sector’s specific critical infrastructure requirements for incidences, threats, and vulnerabilities (PT-ISAC 2016).

Since 1970, FAA officials implemented security measures in response to aviation attacks and foiled plots (see Figure 8). The majority of these measures involved collaboration and leadership from the TSA and are namely enacted post-9/11. These measures include checked baggage screenings and the Federal Air Marshals program on domestic and international flights. The creation of the TSA and DHS was in response to 9/11, as well as the requirements for secondary guarding of cockpit doors and locks, random shoe checks and eventually, all shoe removal, as well as the ban on liquids, the now turned 3-1-1 rule (only three ounces per liquid allowed in carry-on luggage) were after the attempted Shoe Bomber plot. TSA technology screens 100 percent of checked baggage, only physically searching oversized luggage for explosives and suspicious prohibited items (TSA 2016).

Screening technology aids human officers in the security process. TSA’s technology includes millimeter wave advanced imaging technology (AIT) and walk through metal detectors to screen passengers. Automatic technological screening is often preferred over physical screenings, such as pat-downs, by passengers. AIT technology uses automated target recognition software that eliminates passenger-specific images and auto-detects potential threats by indicating their location on a generic outline of a person (TSA 2016).

The issue with TSA’s security measures is that they are almost all in response to attacks or foiled plots. U.S. aviation security is more reactive than proactive, leading to potential budgeting issues and poor cost-benefit analysis. This security implementation focuses on protecting based on the attack, not necessarily the threat. There are currently no responses to the attacks in Brussels and Istanbul, which were largely successful due to the crowding and density created from slow screening and security procedures.

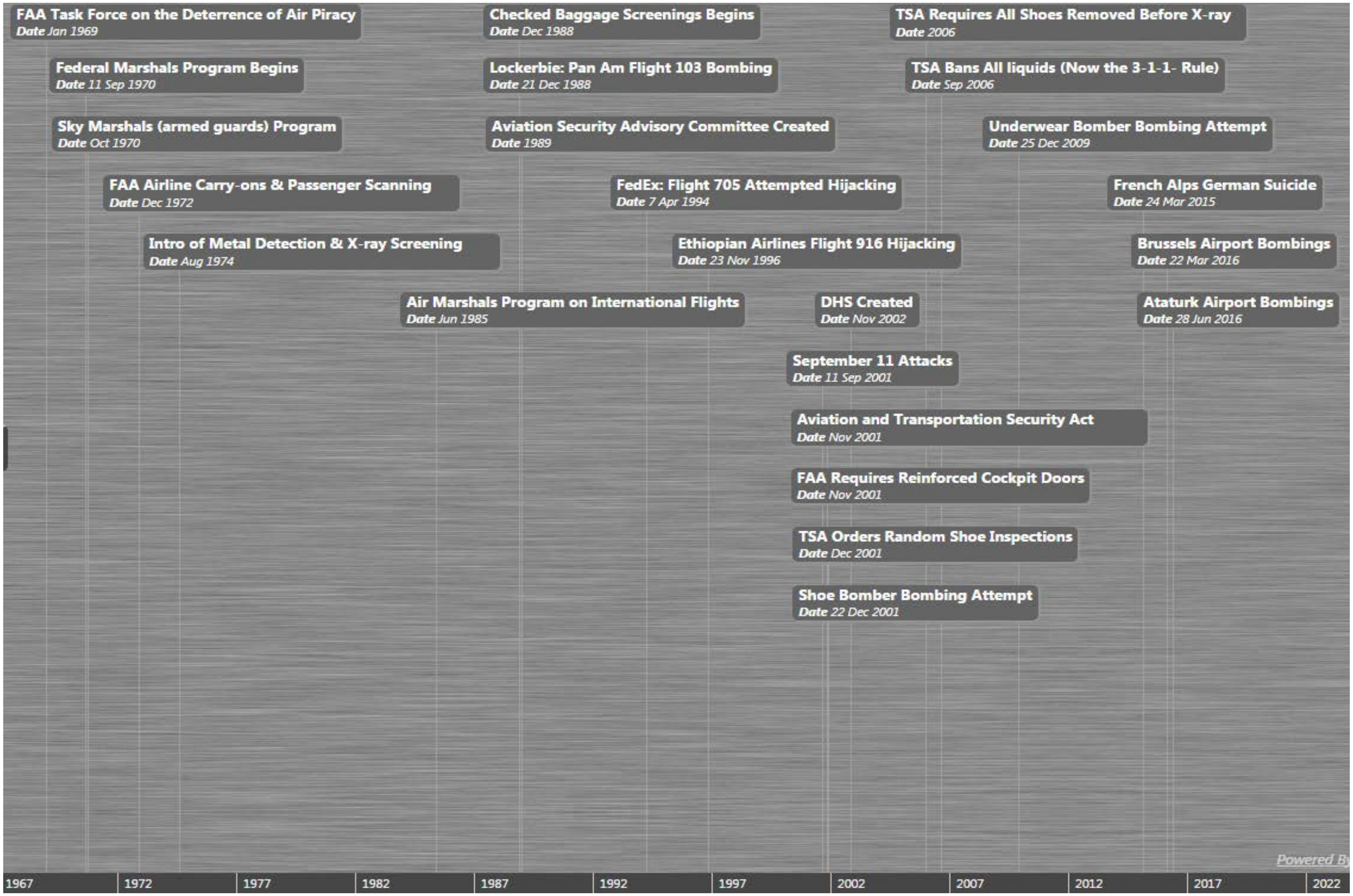

Figure 8. Aviation Security Measures in Relation to Terrorist Attacks
Source: TSA 2016

2.7.1.1 Insider Threat Initiatives

The FAA does not include insider threats in their initiative or program budget (FAA 2015). Although the TSA conducts random employee screening, vetting of new employees, and requires emergency response training, there is an overall lack of aviation insider threat training and awareness. However, in 2015, the Subcommittee on Transportation Security held discussions with TSA, FBI, airport, and airline officials regarding securing the back door in security, instead of focusing solely on the threats from passengers (Homeland Security Committee 2015). This indicates that the insider threat is a concern; however, addressing the threat is in the beginning stages.

2.7.2 Global Aviation Security

Security measures internationally are not uniform. This is likely due to the different nation-state governance and budgeting. In Mexico, aviation security funding is from general revenues. In Canada, it is from airline passenger taxes, which experts argue is an effective tactic because it reduces the burden on treasuries. In the U.S., it comes from public and private contributions. The Aviation Security Infrastructure fee imposed on airlines increases the cost of plane tickets, placing a portion of the burden on passengers (Prentice 2015).

It is likely that international flights pose the greatest threat to U.S. aviation security due to a lack of unification in security measures internationally. Poorer countries, such as Nigeria, lack structured security and the finances needed to match or attempt to match U.S. security. This leads to threats such as the Underwear Bomber. Additionally, aviation terrorist attacks occur more internationally than they do within the U.S.

2.7.3 Train and Bus Security

Attacks in mass transit other than aviation are increasing, rising from about 250 attacks in 2010 to almost 420 in 2015 (GTD 2015). Currently, there are over 200 operational metro rail systems (MRS) globally. Many are under construction and are especially vulnerable to terrorist attacks. The most prevalent weapon used in these attacks by terrorists is explosives. This is due to the ease of smuggling explosives on trains because screening for passengers and checked luggage is rare at stations and the mass casualties that a dense environment could cause (Borrion et al. 2014).

MRS, unlike aviation, lack effective screening, as it is easily penetrable and contains high numbers of people (RAND 2004). Passengers can easily board a train without ever being searched, allowing them to bring items normally prohibited on airplanes onto the trains. In Madrid in 2004, nine bombs in backpacks and other small bags exploded on four different trains at three different stations. Al-Qaeda-inspired terrorists in Spain killed 191 people and injured more than 1,800 (CNN 2016).

Subways present challenges because train schedules are frequent and rapid. In order to screen every passenger and heighten security, the daily routine of millions would be disrupted. The 7 July 2005 London subway bombings also exemplify the lack of security in other forms of mass transit, specifically MRS. Resulting in 52 deaths and over 700 injuries, four suicide bombers attacked three different trains and a double-decker bus. The first bomb killed seven, the second killed six, the third killed 26, and the fourth killed 13. Al-Qaeda claimed responsibility (CNN 2016). In July 2016, an ISIS-inspired teen from Pakistan attacked passengers on a German train with an axe, injuring five people in his suicide-by-police mission. The attacker was a lone wolf who self-proclaimed his allegiance to ISIS. Although ISIS claimed responsibility, officials lack evidence of orders for this attack deriving directly from the group. There are indicators that the teen was planning a “farewell” attack, such as the drawing of the ISIS flag in his room, a suicide note, and a video released by ISIS of the terrorist calling himself a “soldier of the caliphate” (CNN 2016).

Much like that of trains, bus transportation is extremely vulnerable to terrorist attacks. In the U.S., buying a ticket on a Greyhound bus and presenting it to the driver is the only form of security. Passengers can easily carry anything onto the bus, either underneath with the cargo or as carry-on luggage. In 2016, a bus exploded in Jerusalem, killing 21 people. Officials are uncertain whether the lone wolf attacks committed suicide or planted the bomb (LA Times 2016).

These terrorist attacks did not involve insiders. In mass transit, there is less likelihood of an insider threat because 80 percent of attacks are against unprotected targets, such as railroads and buses, making it relatively easy to penetrate existing security and execute an attack (Mineta Transportation Institute 2016). Despite the low risk of insider threats in mass transit, terrorist attacks are still prevalent internationally. In 2015, aviation experienced five terrorist attacks, while all other forms of mass transit saw 420 total (GTD 2015). This is likely due to aviation’s high security level. However, the use of knives in attacks is increasing, as exemplified in the 2015 London subway knife attack (The Guardian 2015), and the 2016 terrorist attack on a train in Germany (BBC 2016).

2.8 Challenges in Protecting Aviation and Mass Transit

There are many challenges in securing aviation and mass transit. Politically, it is difficult to create unification in aviation across all countries. Nations in Africa and the Middle East do not have the political structure to create and implement aviation regulations to U.S. and European standards.

The 2016 Department of Homeland Security budget includes USD 3.7 billion for the TSA under the DHS mission of “Prevent Terrorism and Enhance Security.” The allocated funding is for sustaining aviation security and aligning passenger screening resources based on risk (DHS 2016). A risk-based approach to security assumes that the vast majority of airline passengers present a low risk, the more information known about passengers allows the segmenting of the population in terms of risk, and security will likely increase by focusing more heavily on the unknown and less on known or trusted passengers (Wong and Brooks 2015).

This funding is specific to aviation security, and does not include allocations for securing other mass transit (DHS 2016). Experts argue that stronger cost-benefit analysis is needed to better use these finances (Gillen and Morrison 2015). The U.S. government covers more than twice as much of the TSA’s overall expenditures (see Figure 9). The TSA is experiencing internal issues, including a culture of misconduct. TSA employee told the U.S. House of Representatives that the leadership undermines security. In 2015, checkpoint screeners failed several covert tests to detect “anomalies and potential security threats,” resulting in a newly appointed administrator (LA Times 2016). Employees claim that they had directions to racially profile Somalis in the Minneapolis area(where many Somali-Americans live), were being reassigned to positions out of state after reporting security issues, and witnessed false reports of airport checkpoint lines to make waits appear shorter. This is similar to an insider threat in that it undermines the security of aviation and stems from employees and top leadership.

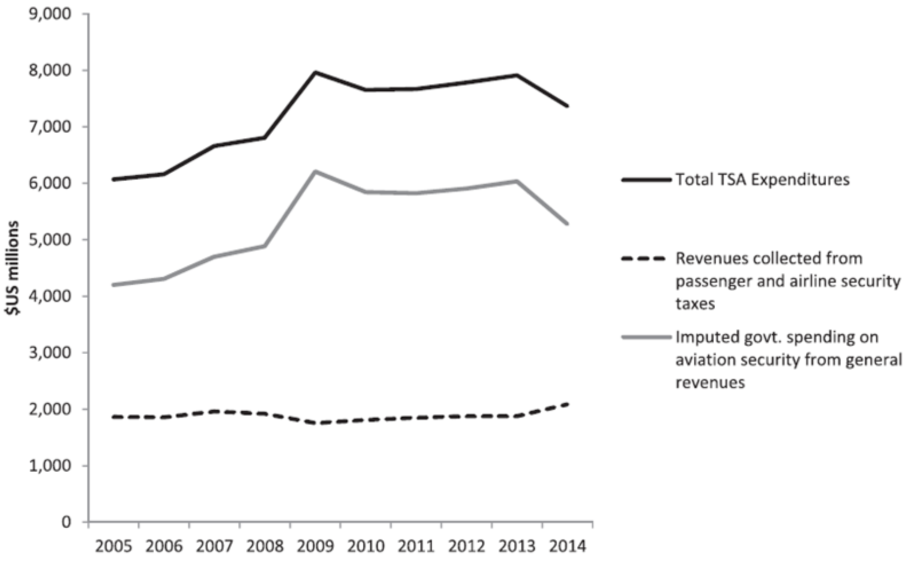

Figure 9. TSA Expenditures 2005-2014
Source: Gillen and Morrison 2015

Security in aviation is often implemented in response to attacks, rather that proactively. This allows terrorists and insiders to evade security, such as the shoe bomber who knew that shoes were not searched at the time of his attempted attack. Afterward, terrorists adapted to new tactics, such as the underwear bomber technique and the use of explosives in cargo. In the case of railroads, trains leave and enter stations so frequently, it is difficult to implement effective and timely security and screening of passengers.

Behavior detection techniques, such as, "questioning, identification of a set of risk factors, and observation" are becoming increasingly popular. These tactics, however, are resource intensive, meaning that they can cost a significant amount of time. Smaller airports may benefit more from behavior detection that international hubs (Wong and Brooks 2015).

One of the greatest challenges in security is privacy concerns. Violating civil rights and privacy for effective security, such as pat-downs and facial recognition, is not favored by the public. Additionally, companies conducting insider threat programs need to be cautious that they are not violating the privacy of their employees by looking for behavioral indicators that may involve personal information beyond the limits of human resource needs (Greitzer et al. 2010).

Another issue for passengers is waiting in long lines to go through security. This brings to light the tradeoff of convenience for security. Airport security wait times are inevitable, however the DHS is increasing the use of overtime to increase the number of screening officers in efforts to alleviate wait times (CNN 2016). The TSA recommends arriving up to two hours prior to flights. These long lines create another target for terrorists that does not require passing through security to access. A heavily populated area prior to security is a vulnerable target, as displayed in the Brussels and Istanbul airport attacks in 2016.

Finally, the aviation industry relies heavily on technology, from screening machines to Wi-Fi onboard aircraft. There are likely cyber vulnerabilities in this equipment and machines, such as the facial recognition technology in Malaysia, which insiders and terrorists can exploit (see Section 2.10.4). The human problem of terrorism requires human solutions in conjunction with technology.

2.9 Effective and Ineffective Security Measures

The TSA claims that in its layered security approach (see Figure 10), “each one of the layers alone is capable of stopping a terrorist attack. In combination their security value is multiplied, creating a much stronger, formidable system. A terrorist who has to overcome multiple security layers in order to carry out an attack is more likely to be pre-empted, deterred, or to fail during the attempt” (TSA 2014, in Jackson and LaTourrette 2015). This system has security and social benefits; however, it also has weaknesses.

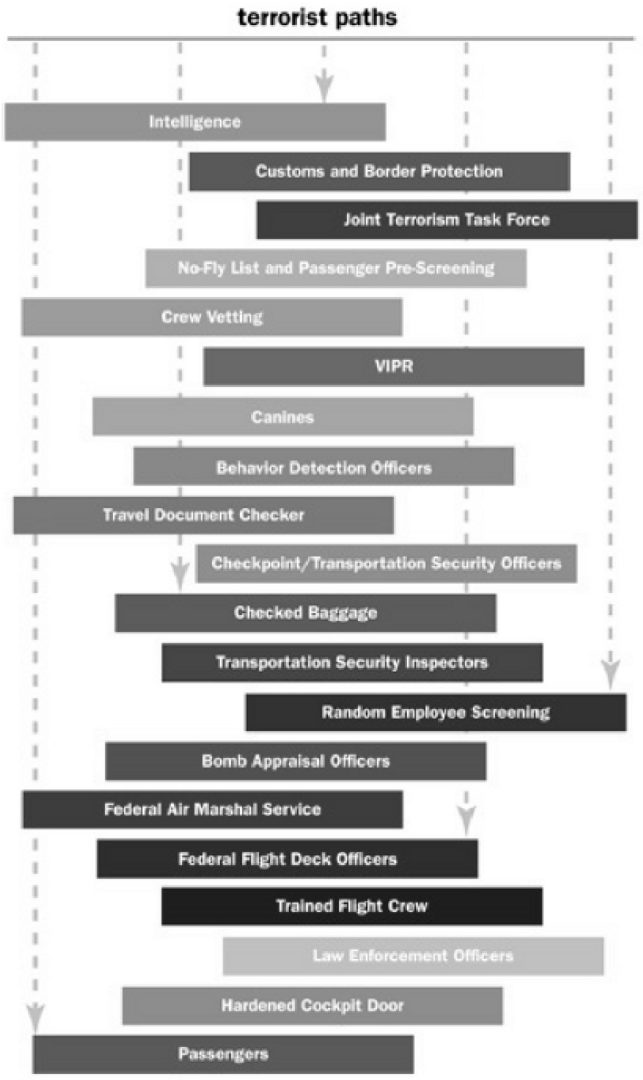
terrorist paths
Intelligence
Customs and Border Protection
Joint Terrorism Task Force
No-Fly List and Passenger Pre-Screening
Crew Vetting
VIPR
Canines
Behavior Detection Officers
Travel Document Checker
Checkpoint/Transportation Security Officers
Checked Baggage
Transportation Security Inspectors
Random Employee Screening
Bomb Appraisal Officers
Federal Air Marshal Service
Federal Flight Deck Officers
Trained Flight Crew
Law Enforcement Officers
Hardened Cockpit Door
Passengers

Figure 10. TSA Layered Security
Source: TSA, in Jackson and LaTourrette 2015

Four avenues for a terrorist attack exist: passenger entry to the system, employee entry, the baggage or cargo system, and covert entry to the airport through climbing a fence or breaking in (Jackson and LaTourrette 2015). The TSA focuses heavily on security measures relevant to the passenger entry avenue, such as intelligence, customs and border protection, the No-Fly list, behavior detection officers, and Federal Air Marshals. However, the TSA presents fewer types of layers to protect other avenues, such as insider threats through employee entry. The known measures that exist include crew vetting, random employee screening, and trained flight crew (TSA 2014, in Jackson and LaTourette).

Implementing multiple security layers that function differently provides increased public confidence that there is complete coverage for a specific path. However, officials continue to debate over the cost-effectiveness of multiple layers. A cost-benefit study found that compared to other security measures, such as locked cockpits, armed pilots, and secondary cockpit barriers, Federal Air Marshals are a "very poor investment." This poor performance derives from their high annual cost and the small amount of flights where they are present. Eliminating Federal Air Marshals would save the U.S. about USD 820 million annually (Stewart and Mueller 2012, in Poole 2015). TSA PreCheck, designed to let fliers use an expedited screening line if they submit a government background check, is also ineffective. It has fallen short of reaching its goal of 25 million passengers and uses many TSA resources for a small group of people. Only 7.3 million passengers use the program. Despite its shortcoming, largely due to poor advertisement of the program, the TSA is planning to spend USD 1.9 million on promotion in 2016 (LA Times 2016).

In contrast, cockpit locks and secondary barriers likely reduce the number of hijackings, a popular method of attack before 9/11 (GTD 2015). Post-September 11 hijacking attacks, the TSA requires these extra measures to secure pilots and passengers. However, a caveat with mistrust for pilots within the closed-off cockpits exists. In 2015, the Germanwings co-pilot locked his partner out of the cockpit while using the restroom. He was then able to hijack the aircraft, ultimately crashing it into the French Alps. Additionally, random security checks are a useful tool in detecting unknown threats. For example, if these measures were in use at the checkpoint that the attempted shoe bomber passed through, there would have been no guarantee for him that he would make it through security, potentially deterring him.

Having multiple layers increase the number of humans involved in the security process, likely increasing the number of potential insider threats within airports and airlines. Additionally, "if a new detection technology is added that produces many false alarms that security personnel have to spend time resolving, that may reduce their effectiveness in observing and detecting threats on their own" (Jackson and LaTourrette 2015). The inside-out approach to security involves beginning with the worst possible outcome, and working back to make that scenario unlikely. This includes creating barriers to prevent catastrophic events like 9/11 from happening. In contrast, aviation security today works in an outside-in problem solving approach in which security officials identify the core issue or specific threat from an outside perspective. Security is then implemented to stop that particular threat, such as prohibiting firearms and explosives on aircraft in response to intelligence that an attacker wishes to blow up an airplane (Hawley DHS 2009).

Additionally, the standard operating procedures executed by technology consistently produce the same results. This may prevent human intuition from stepping in and allowing security officers to think and adjust in real time, which is an advantage over machines. The human advantage is seen in human senses and ability to detect subtle clues that something is wrong (Hawley DHS 2009). Former TSA Administrator Kip Hawley claims that successful security involves trade-offs. Officials should take what they know to guard against the known threat, while also guarding against the unknown threat that may evade standard procedures (Hawley DHS 2009).

2.10 Looking Forward

2.10.1 Politically

President Obama's Executive Order 13587 establishes the National Insider Threat Task Force, which aims to, "deter, detect, and mitigate actions by employees who may represent a threat to national security by developing…policy, standards, guidance, and training." The DHS, which the TSA is part of, is involved in this task force (NITTF 2011). This is likely a beneficial starting point for the TSA and the rest of the industry in implementing insider threat initiatives. There is also a need for international policy and at least partial unification of regulations and standards regarding security. This will likely reduce the threat of terrorist events impacting international flights.

2.10.2 Economically

The TSA should allocate part of its budget toward insider threat training and awareness programs. Periodic training and covert tests in airports will benefit airlines and aviation security alike. Investing in the prevention of a catastrophic, insider-related terrorist attack will likely be cost-beneficial in the long run. Additionally, TSA intends to hire 768 new employees in order to reduce security wait times and balance crowd size may not be beneficial (CNN 2016). Adding more employees is ineffective if more security lines are not added. This leaves room for more human error, malicious intent, and vulnerabilities. Training existing employees to correctly detect and address insiders will improve the quality of security, rather than focusing on the quantity of employees.

2.10.3 Physically

Aside from TSA's random employee screenings and vetting of new employees, training and awareness in the behavioral indicators of insider threats should become part of TSA's requirements. With an increase in reliance on technology and the potential for human error and malicious intent, education will likely aid in employees' and employers' understanding of the threats and allow them to better detect and address them.

The TSA and American Airlines are partnering to launch new checkpoints worth USD 5 million that will likely cut passenger wait times up to 30 percent. The agency plans to implement two new lines at the Los Angeles, Chicago O'Hare, Dallas/Fort Worth, and Miami International Airports. These new checkpoints include two conveyor belts, one that sends empty plastic bins to waiting passengers and one that moves filled bins toward the X-ray machines. Officials expect this to allow lines of passengers to continue moving despite random selections for extra screenings (LA Times 2016). Pending positive results, it is likely that these lines will appear in an increasing number of airports across the U.S.

U.S. airport executives and policymakers are debating the implementation of Israeli airport security measures into U.S. airports due to the country's layers of security at Ben Gurion airport resulting in preventing hijackings and terrorist attacks at the facility for over 46 years (Security InfoWatch 2016). Measures used in Israel include extensive passenger profiling based on behavior and appearance, which is widely accepted by the Israeli public. Multiple security screenings, similar to that in the U.S., include screenings passengers again when they reach their terminals.

Despite the likelihood of successful results if the U.S. fully implements Israeli tactics, TSA administrator Peter Neffenger claims that there will likely be an increase in ticket prices to pay for extra screening measures, as well as longer wait times. Ben Gurion travelers arrive at least three hours ahead of time, while the TSA recommends up to two hours. Another argument against these measures in the U.S. is the "risk versus return on investment" (Security InfoWatch 2016).

2.10.4 Further Research: Cyber Capabilities, Terrorism, and the Insider Threat

As exemplified in the Malaysian breach discovered in early 2016, insider threats through cyberspace are increasing. Much of the aviation industry relies on technology in screening, verification, the aircraft, communications, and Wi-Fi onboard. All of these present vulnerabilities can be accessed by malicious actors. It is highly unlikely that terrorists have significant cyber capabilities. In contrast, this increases the likelihood of unintentional insiders being exploited, as well as the chances of insiders working in aviation abusing their system privileges to sell data to terrorists or provide themselves with unauthorized access. Additionally, analyzing the potential cyber indicators of insider threats will likely assist employees and employers in detecting threats and preventing a breach similar to that in Malaysia. This topic is beyond the scope of this report; however, cyber is a growing field of research and exploitation and should be addressed regarding insider threats and terrorism in airports and aircraft. Another topic for future discussion regards the economic benefit of airlines managing security and creating their own insider threat programs. Airlines will likely profit more from privatized security funding, rather than partial government funding. Airline involvement presents the opportunity for improved security processes.

3.0 Conclusion

Aviation will continue to be a terrorist target due to its economic value and the opportunity for an international stage while causing mass casualties. Several previous attacks indicate that insider threats in aviation are increasing, such as the Lockerbie bombing, the FedEx attempted hijacking, and the Germanwings co-pilot suicide in the French Alps. Attacks on aviation typically include explosives and many attacks involve suicide missions. Lone wolves acting maliciously typically commit suicide, using the aircraft as the weapon. Indicators and warnings of these attacks, and others, exist, along with indicators of insider activity in certain events. Understanding previous aviation insider threat events will likely aid in stimulating proactive security measures, rather than reactive responses. Despite many layers of security in place protecting against threats from passengers, there is room for improvement in securing against the insider threat. The industry lacks insider threat initiatives and heightened security training and awareness against malicious employees. Reactive security measures narrow the scope of potential attacks by focusing on known threats, rather than proactively securing against unknown threats.

Compared to other mass transit, including trains and buses, aviation is secure and has a lower risk of experiencing a successful attack. Train passengers are four times more likely to experience a terrorist attack than those traveling by aviation (Express UK 2015). Railroads, subways, and buses do not require thorough passenger screening or luggage scanning, making it relatively easy for terrorists to attack civilian transportation, as seen in the 2016 German attacks. There are many challenges in securing aviation, such as privacy concerns, long lines that create large, vulnerable targets, a lack of international security uniformity, and internal issues at the TSA. Improving global security standards for international flight security will likely reduce the threat of a terrorist attack in the U.S. Implementing insider threat programs and following guidelines set by the National Insider Threat Task Force will aid in reducing malicious insider activity by appropriating part of TSA's budget toward training and awareness, instead of toward proven ineffective security measures, such as Federal Air Marshals. Post 9/11, security measures improved and the U.S. has not experienced a similar attack. Addressing the insider in aviation terrorism is necessary, as it is an increasing threat to the safety of civilians. Understanding this threat will likely mitigate the likelihood of a successful domestic aviation attack involving an insider.

4.0 References

ABC News. 2012. “Stink Bomb: Underwear Bomber Wore Explosive Undies for Weeks, FBI Says.” Accessed July 18, 2016 at http://abcnews.go.com/blogs/headlines/2012/09/stink-bomb-underwear-bomber-wore-explosive-undies-for-weeks-fbi-says/

Abrahms M. 2008. “What Terrorists Really Want: Terrorist Motives and Counterterrorism Strategy.” In International Security, pp. 77-105. MIT Press, Massachusetts Institute of Technology, Cambridge, Massachusetts.

Aviation Benefits. 2016. “Value to the economy.” Accessed July 20, 2016 at http://aviationbenefits.org/economic-growth/value-to-the-economy/

BBC. 2016. “9/11 and the road to war.” Accessed July 20, 2016 at http://www.bbc.co.uk/history/events/the_september_11th_terrorist_attacks

BBC. 2005. “1970: Hijacked jets destroyed by guerrillas.” Accessed July 18, 2016 at http://news.bbc.co.uk/onthisday/hi/dates/stories/september/12/newsid_2514000/2514929.stm

Borrion H, K Tripathi, P Chen, and S Moon. 2014. “Threat detection: a framework for security architects and designers of metropolitan rail systems.” In Urban Planning and Transport Research, pp. 1-23. Routledge, U.K.

CERT. 2016. “Overview: Insider Threat.” Accessed July 25 at http://www.cert.org/insider-threat/

CNN. 2016. “TSA security line waits inevitable, DHS secretary says.” Accessed July 25, 2016 at http://www.cnn.com/2016/05/13/aviation/tsa-long-lines-us-airports/

CNN. 2016. “Spain Train Bombings Fast Facts.” Accessed July 25, 2016 at http://www.cnn.com/2013/11/04/world/europe/spain-train-bombings-fast-facts/

CNN. 2016. “ISIS-inspired teen who attack German train passengers, official says.” Accessed July 25, 2016 at http://www.cnn.com/2016/07/20/world/germany-train-attack/index.html

CNN. 2016. “Istanbul airport attack: 36 dead, 147 injured, Turkish officials say.” Accessed July 18, 2016 at http://www.cnn.com/2016/06/28/europe/turkey-istanbul-airport-attacks/

CNN. 2016. “July 7 2005 London Bombings Fast Facts.” Accessed July 25, 2016 at http://www.cnn.com/2013/11/06/world/europe/july-7-2005-london-bombings-fast-facts/

CNN. 2015. “Germanwings Flight 9525 co-pilot suicidal at one time, prosecutor says.” Accessed July 18, 2016 at http://www.cnn.com/2015/03/30/europe/france-germanwings-plane-crash-main/

CNN. 2015. “Two Libyans identified as Lockerbie bombing suspects, Scotland, U.S. say.” Accessed July 29, 2016 at http://www.cnn.com/2015/10/15/europe/lockerbie-pan-am-flight-103/

CNN. 2013. “Pan Am Flight 103 Fast Facts.” Accessed July 18, 2016 at http://www.cnn.com/2013/09/26/world/pan-am-flight-103-fast-facts/

Crenshaw Martha. 1998. “The logic of terrorism: Terrorist behavior as a product of strategic choice.” Chapter 1 in Origins of Terrorism, ed. W Reich, Baltimore, Maryland.

DHS. 2016. “Fact Sheet: Department of Homeland Security Fiscal Year 2016 Budget.” Accessed July 25, 2016 at https://www.dhs.gov/news/2015/02/02/fact-sheet-dhs-fy-2016-budget

FAA. 2015. “FAA Strategic Initiatives.” Accessed July 24, 2016 at https://www.faa.gov/about/plans_reports/media/FAA_Strategic_Initiatives_Summary.pdf

Fitsanakis J. 2016. “Malaysia immigration probe reveals growing insider threat to passport security.” Intel News. Accessed July 21, 2016 at https://intelnews.org/2016/06/03/01-1914/?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+intelNewsOrg+%28intelNews.org%29

Ford W. 2015. “Education & Awareness: Manage the Insider Threat.” Accessed July 18, 2016 at http://csrc.nist.gov/organizations/fissea/2015-conference/presentations/march-24/fissea-2015-willis-ford.pdf

Gearson J. 2002. “The Nature of Modern Terrorism.” In The Political Quarterly Publishing Co., pp. 7-24. U.K.

Gillen D and WG Morrison. 2015. “Aviation security: Costing, pricing, finance and performance.” In Journal of Air Transport Management, pp. 1-12. Amsterdam, Netherlands.

Global Terrorism Database. 2016. “Codebook: Inclusion Criteria and Variables.” The National Consortium for the Study of Terrorism and Responses to Terrorism. University of Maryland, College Park, Maryland.

Global Terrorism Database. 2016. “Transportation Incidents over Time.” The National Consortium for the Study of Terrorism and Responses to Terrorism. University of Maryland, College Park, Maryland. Accessed July 25, 2016 at https://www.start.umd.edu/gtd/search/Results.aspx?search=transportation&sa.x=0&sa.y=0&sa=Search

Greitzer FL, AP Moore, DM Cappelli, DH Andrews, LA Carroll, and TD Hull. 2007. “Combating the Insider Threat.” In IEEE Security and Privacy, pp. 61-64.

Greitzer FL, LJ Kangas, CF Noonan, CR Brown, and T Ferryman. 2014. “Psychosocial Modeling of Insider Threat Risk Based on Behavioral and Word Use Analysis.” e-Service Journal, pp. 106-138. Indiana University Press, Indiana University, Bloomington, Indiana.

Greitzer FL, LJ Kangas, CF Noonan, and AC Dalton. 2010. “Identifying at Risk Employees: A Behavioral Model for Predicting Potential Insider Threats.” Pacific Northwest National Laboratory, Richland Washington.

Hawley K. 2009. “The Underwear Bomber: A Case Study of Inside-Out Risk Management.” Accessed July 25, 2016 at https://www.chds.us/coursefiles/cip/lectures/transportation/cip_underwearbomber/player.html

Homeland Security Committee. 2015. “TSA, FBI, Airport & Airline Industries Discuss Insider Threats.” Accessed July 24, 2016 at https://homeland.house.gov/press/tsa-fbi-airport-airline-industries-discuss-insider-threats

Institute for the Analysis of Global Security. 2004. “How much did the September 11 terrorist attacks cost America?” Accessed July 20, 2016 at http://www.iags.org/costof911.html

Jackson BA and T LaTourrette. 2015. "Assessing the effectiveness of layered security for protecting the aviation system against adaptive adversaries." *Journal of Air Transport Management*, pp. 26-33. Amsterdam, Netherlands.

Lewis S. 2016. "Malaysian Immigration Officials Have Been 'Sabotaging' Airport Security for Year." In Time Magazine. Accessed at http://time.com/4353235/malaysia-immigration-sabotage-criminals

Los Angeles Times News. 2016. "TSA an 'agency in crisis' with leadership undermining security, employees tell Congress." Accessed July 25, 2016 at http://www.washingtontimes.com/news/2016/apr/27/tsa-employees-tell-house-panel-poor-leadership-ret/

Los Angeles Times News. 2016. "TSA and American Airlines to launch new checkpoints to cut wait times up to 30%." Accessed July 24, 2016 at http://www.latimes.com/business/la-fi-tsa-checkpoint-20160705-snap-story.html

Los Angeles Times News. 2016. "Jerusalem bus explosion that wounded at least 21 was a terror attack, police say." Accessed July 25, 2016 at http://www.latimes.com/world/la-fg-jerusalem-explosion-20160418-story.html

Los Angeles Times News. 2016. "Why hasn't TSA PreCheck reduced airport wait times?" Accessed July 25, 2016 at http://www.latimes.com/business/la-fi-tsa-precheck-20160527-snap-story.html

Mineta Transportation Institute. 2016. "Preliminary Thoughts on the Role of Insiders in Attacks on Transportation Targets." Accessed July 24, 2016 at http://transweb.sjsu.edu/PDFs/research/role-of-insiders-in-terrorist-attacks-on-transportation.pdf

National Commission on Terrorist Attacks Upon the United States.2004. "9-11 Commission Report."

National Consortium for the Study of Terrorism and Responses to Terrorism (START). 2016. Global Terrorism Database. Accessed July 20, 2016 at https://www.start.umd.edu/gtd/

National Counterintelligence and Security Center (NCSC). 2011. National Insider Threat Program. Accessed July 18, 2016 at https://www.ncsc.gov/nittf/docs/National_Insider_Threat_Policy.pdf

NBC News. 2015. "Shoe-Bomber Has 'Tactical Regrets' Over Failed American Airlines Plot." Accessed July 18, 2016 at http://www.nbcnews.com/news/us-news/shoe-bomber-has-tactical-regrets-over-failed-american-airlines-plot-n296396

Newswire. 2015. "Remembering Hijacked Flight 705 That Flew Upside Down." Accessed July 18, 2016 at http://newswire.net/newsroom/news/00090795-fedex-flight-705.html

PBS. 2009. "Hijacked." Accessed July 29, 2016 at http://www.pbs.org/wgbh/amex/hijacked/

Poole Jr. RW. 2015. "Fresh thinking on aviation security." In Journal of Air Transport Management, pp. 65-67. Amsterdam, Netherlands.

RAND Corporation. 2004. "Terrorism and Rail Security." Accessed July 2015 at http://www.rand.org/content/dam/rand/pubs/testimonies/2005/RAND_CT224.pdf

Ross B, R Schwartz, and M Chuchmach. 2011. “New Terror Report Warns of Insider Threat to Utilities.” ABC News. Accessed July 20, 2016 at http://abcnews.go.com/Blotter/terror-alert-warns-insider-threat-infrastructure/story?id=14118119

Security InfoWatch. 2016. “Can Israeli-type security measures wok at U.S. airport?” Accessed July 25, 2016 at http://www.securityinfowatch.com/news/12234607/can-israeli-type-security-measures-work-at-us-airports

START - Study of Terrorism and Responses to Terrorism. 2016. Accessed July 29, 2016 at https://www.start.umd.edu/

The Guardian. 2010. “Cargo plane bomb found in Britain was primed to blow up over U.S.” Accessed July 18, 2016 at https://www.theguardian.com/world/2010/nov/10/cargo-plane-bomb-us-alqaida

The National Security Archive. 2001. “Bin Ladin Determined to Strike in U.S.: PDB.” Accessed July 18, 2016 at http://nsarchive.gwu.edu/NSAEBB/NSAEBB116/pdb8-6-2001.pdf

TrendMicro. 2016. “Hackers get more targeted with recent spear phishing campaigns.” Accessed July 20, 2016 at http://blog.trendmicro.com/hackers-get-more-targeted-with-recent-spear-phishing-campaigns/

TSA. 2016. “Mission.” Accessed July 24, 2016 at https://www.tsa.gov/about/tsa-mission

Wong S and N Brooks. 2015. “Evolving risk-based security: A review of current issues and emerging trends impacting security screening in the aviation industry.” In Journal of Air Transport Management, pp. 60-64. Amsterdam, Netherlands.

Appendix A

Additional Case Study Data

Table A.1. Additional Information on Aviation Attack Case Studies (Source: GTD 2015)

Date	Attack	Airline	Location	Country	Region	Classification	Perpetrators (Affiliation)	Number of Perpetrators	Perpetrator Gender (F/M)	Deaths	Target
6-Sep-70	Dawson's Field	TWA Flight; Swissair; El Al; Pan Am	European Airports-Zarqa	Europe-Jordan	Middle East	Hijackings	Popular Front of the Liberation of Palestine (PFLP)	8	F: 1 M: 7	1	Airports and aircraft
21-Dec-88	Pan Am Flight 103	Pan Am	Lockerbie	Scotland	Western Europe	Bombing/Explosion	Unknown; Libyan Abdel Basser Ali al-Megrahi convicted; Libyan Lamen Khalifa Fhimah acquitted; Libyan Prime Minister Gaddafi and government	2	M: 2	270	Airports and aircraft, private citizens and property
7-Apr-94	FedEx Flight 705	FedEx	Memphis, TN	US	North America	Armed Assault	Lone wolf: Auburn Calloway	1	M: 1	0	Airports and aircraft, private citizens and property
23-Nov-96	Ethiopian Airlines Flight 916	Ethiopian Airlines	Addis Ababa	Indian Ocean	Sub-Saharan Africa	Hostage taking	Lone wolves seeking asylum in Australia	3	M: 3	123	Airports and aircraft
11-Sep-01	American Airlines Flights 11 and 77; United Airlines Flights 175 and 93	American Airlines; United Airlines	New York City, NY; Arlington, VA; Shanksville, PA	US	North America	Hijackings	Al-Qaeda	19	M: 19	2,997	Airports and aircraft, government, military, private citizens and property
22-Dec-01	Shoe Bomber American Airlines Flight 63	American Airlines	Paris-Miami	France-US	Western Europe-North America	Failed Bombing/Explosion	Al-Qaeda: Richard Colvin Reid	1	M: 1	0	Airports and aircraft, private citizens and property
25-Dec-09	Underwear Bomber	Northwest Airlines	Detroit	US	North America	Failed Bombing/Explosion	Al-Qaeda: Umar Farouk Abdulmutallab	1	M: 1	0	Airports and aircraft
29-Oct-10	UPS Cargo Planes Ink Cartridge Bombing Plot	UPS	Sana'a	Yemen	West Asia	Bombing/Explosion	Al-Qaeda in the Arabian Peninsula (AQAP)	N/A	N/A	0	Airports and aircraft
24-Mar-15	German Suicide	Germanwings	French Alps	France	Western Europe	Hijacking	Lone wolf: Andreas Lubitz	1	M: 1	150	Airports and aircraft
22-Mar-16	Brussels Airport Bombings	N/A	Brussels	Belgium	Western Europe	Bombing/Explosion, Armed Assault	ISIS	3	M:3	32	Airports and aircraft
28-Jun-16	Ataturk Airport	N/A	Istanbul	Turkey	West Asia	Bombing/Explosion, Armed Assault	ISIS	3	M:3	42	Airports and aircraft, private citizens and

Pacific Northwest
NATIONAL LABORATORY

U.S. DEPARTMENT OF
ENERGY

Proudly Operated by Battelle *Since 1965*

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99352
1-888-375-PNNL (7665)

www.pnnl.gov