

**Security vs. Efficiency:
Assessing Transportation Security Policies and Trade-Offs**

Anna Arciszewska
Jessica Horning
Patrick Phenow
Ryan Wilson

CE 5212
Transportation Policy, Planning, & Deployment
Prof. David Levinson
September 14, 2007

Introduction

Security and efficiency have long been trade-offs in the world of passenger and freight mobility. The security of products and people, whether it is physical screening or requirements for the transportation of hazardous materials, requires time, money, and manpower. Efficiency, the ability to move products and people with the least amount of delay, requires different types of investments of time, money, and manpower. Establishing a balance between security and efficiency has always been a difficult job for the legislators, regulators (executive branch), and the regulated (special interest groups and businesses).

The trade-off debate grew quickly in the wake of the terrorist attacks on September 11th when new questions about security arose. Legislators were quick to act, enacting legislation that created, among other things, the Department of Homeland Security and associated Transportation Security Administration. Security tightened, particularly at airports. Critics of these actions were no further behind in establishing their case, asserting the new security measures are overly restrictive resulting in unnecessary inefficiencies.

As this paper will discuss, the argument remains an issue of trade-offs. In a world of limited time, money, and resources affording both the best security and highest efficiency isn't practical and likely not possible. Strong emotions, staunch supporters, value-laden arguments, and empirical evidence fill each side of the debate. Perhaps unsurprisingly, a security/efficiency balance point remains undefined. Equally unclear are the terms or performance measures that might be used to reach the balance point.

An examination of security and efficiency could occur in several contexts. This report focuses solely in the field of transportation, discussing both freight/non-airline security and airport/airline security. We will discuss and weave freight/non-airline issues and evidence throughout, but focus more heavily on airports. Freight concerns are important but security responses have been fewer in number and less rapid in deployment, limiting the number of sources.

We begin by discussing the history of transportation security in the United States, focusing on airports and the TSA. History assists in framing the current issues of the security/efficiency debate. Together these sections illustrate how the maturity of the current transportation security system has been predominantly a reactive process and that new policy approaches are needed to address current inefficiencies in the system (i.e. airline security systems characterized by a single point of failure). Current issues also lend to a number of other discussion points, including the idea of "security theater." We continue with an examination of relevant research and case studies examining a range of tradeoffs. Among them, the efficiency of investment in technology versus people and the efficiency of investment in specific types of attacks versus general emergency preparedness. We also examine theory and empirics of recent investments in the U.S. and abroad. Discussions of this type continue to be important for legislators, the regulators, and the regulated due to its impact on personal safety, product prices, and large recent capital investments.

History

United States transportation security has been a subject of intensive discussion the past several years. Without question the events of September 11, 2001 have led to increased focus on airline security and traveler's safety worldwide. The U.S. has been at the forefront of such discussion and deployed the most drastic changes in air transportation security, aimed at protecting American's from terrorism.

Interest in securing U.S. airlines began far before 9/11. Hick jacking became an issue in the 1960's and 1970's and the banning of guns on planes was an immediate response. Security agents were limited at that time to checking whether the passenger had a gun and asking questions about their baggage. Still familiar to traveler's today, years before 9/11 there was a ticket agent who checked a person's photo ID and a security agent checking for weapons and asking 'who and when packed your baggage?', 'did you received anything from a stranger?', 'did you leave your bag unattached at any time?' Each airport had its private security that provided safety for American citizens.

As security evolved the airport personnel started employing x-ray machines to detect banned objects at security checkpoints. This technology prompted the federal government to collect statistics on screening performance. The United States Government Accountability Office in its report on aviation security from May, 2005 states,

“In 1978, screeners failed to detect 13 percent of the potentially dangerous objects that Federal Aviation Administration (FAA) agents carried through airport screening checkpoints during tests. In 1987, screeners did not detect 20 percent of the objects in similar tests. In tests conducted during the late 1990s, as the testing objects became more realistic, screeners' abilities to detect dangerous objects declined further” (United States Government Accountability Office 2005, pg. 12)

Advancements in screening technology did not stop the September 11 terrorist attacks, a harsh wake-up call for security agencies and the federal government. In rapid response, President George W. Bush signed the Aviation and Transportation Security Act on November 19, 2001. At this point, the newly created federal Transportation Security Administration (TSA) became the sole agency in charge of securing over 450 commercial airports (United States Government Accountability Office 2005).

Regulation and restrictions concerning carry-on baggage have changed dramatically. For a period following 9/11 the federal government banned all carry-on baggage. Every passenger and all checked baggage was scanned for explosive items. Cigarette lighters and sharp objects were not allowed onboard. The meals served on the plane included plastic cutlery. The TSA also implemented the Passenger Name Record. Airline Security was cooperating with government agencies to “identify individuals on passenger lists who may be a threat to security and notify law enforcement agencies to prevent them from boarding” (International Air Transport Association 2006).

Future threats prompted further restrictions and regulations. In response to Richard Reid's attempt to conceal a bomb in his shoes, the TSA required passengers to remove their shoes and

run them through the x-ray scanner. Coats, jackets, and certain belts quickly followed. The TSA introduced additional changes in August 2006. All liquids and gels had to be removed from the carry on baggage after a terrorist attack attempt in London, UK. The current standard restricts gels and liquids to 3oz bottles and their total space to a single quart plastic bag.

The changes implemented by TSA post-9/11 have had a range of impacts. The first is cost as approximately \$6 billion is spent annually on airline security. The second is efficiency. Passengers are required to check-in at least 75 minutes prior to departure for a domestic flight and 2 to 3 hours prior to an international flight. Inefficiencies grew at the airport as well. Screening lines grew and stalled as passengers carrying prohibited items such as cigarette lighters and bottled water required additional checks. Some passengers traveling shorter distances choose now chose road travel instead. The decrease in passenger travel resulted in a airline loss of \$13 billion in 2001 and \$11 billion in 2002. Losses in those years were the most dramatic in terms of airline loss due to security inefficiency. According to International Air Transport Association, improvement in the security efficiency reduced losses to slightly over \$3 billion in 2005 (International Air Transport Association 2006).

Current Issues & Context

The current issues in the security/efficiency debate are numerous in number and wide in scope. Making a case for obtaining and maintaining both secure and efficient systems isn't necessary as the opposite, insecure and inefficient, is not desirable. Security and efficiency have associated costs and the trade-offs of these costs and their related benefits remain a contentious point of debate. Stemming from the attacks on September 11th, few would argue terrorism has been the most frequent item of discussion. The Bush Administration has placed counterterrorism at the top of its agenda. As a result of these actions, a number of responses and related issues have emerged:

- 1) A reexamination and restructuring of transportation security and safety policies and procedures in response to terrorism risks,
- 2) The difficulty of deploying security measures for all modes of transportation with inadequate funding.
- 3) An increase in liability for private firms providing security services,
- 4) How to achieve a balance between greater security and high levels of movement and access for products and people,
- 5) The role of the Department of Homeland Security and the separation of responsibilities at each level of government (Johnston and Nath 2004).

In the world of transportation, these actions have placed more emphasis on security in place of efficiency. For example, containerization of freight improved the efficiency of intermodal transportation. However, the possibility of terrorist attacks at intermodal freight terminals and subsequent security measures have tempered the efficiencies gained through containerization (Johnston and Nath 2004).

The key issue remains defining, achieving, and obtaining a security/efficiency balance. Most pundits on both sides of the debate will acknowledge a greater push for efficiency prior to 9/11.

Johnston argues that society must shift from an efficiency based system to one that strikes a balance between efficiency and security. This rebalancing act will require focus, will, skill, and money (Johnston 2004).

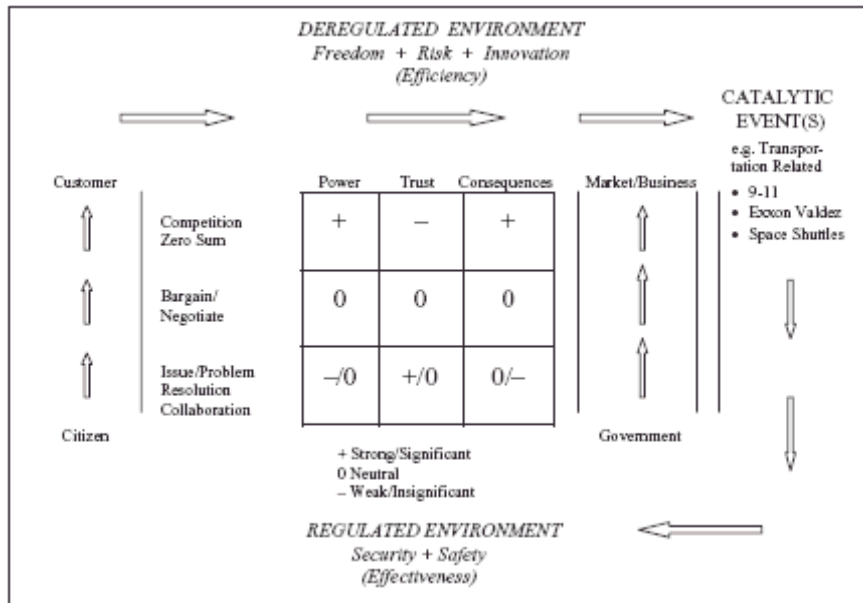


FIGURE 1: The Emerging Entrepreneurial Management and Public Policy Model; from (Johnston 2004, pg. 268)

Figure 1 visually explains the shift in efficiency and security discussed in the Johnston article. Johnston asserts a shift from security and safety, the bottom of the model, to efficiency and greater risk, the top of the model, occurred prior to 9/11. The left axis lists problem/issue resolution strategies as a system moves from security to efficiency. A catastrophic event, such as 9/11 results in a shift downward from efficiency to effectiveness (security) (Johnston 2004). This model helps to demonstrate the relationship of public policy, market forces, efficiency and security and the role of events such as 9/11 in altering these relationships.

This type of situation unarguably exists in the airport realm but the same arguments apply to other modes as well. In the context of maritime port security, a large sum of money has been invested in port security since 9/11. The shipping industry, like airlines, is having a difficult time establishing a balance between security and efficiency. Intermodal ports are highly susceptible to terrorism among other risks including product theft and worker safety. The cost of upgrading ports beyond recent security expenditures could be significant and perhaps impossible for some businesses. Reiterating an earlier point; containerized cargo had a huge impact on the efficiency of freight movement, impacting global trade, economics of scale in production, intermodal capabilities, and operations integration. The time and the resources needed to achieve additional security measure have direct impacts on system cost, speed, and resultant efficiency (Khalid 2006).

Another perspective on this debate is the idea of risk management. Ericson sets the context in a recent article. In any system, risk is the probability of harm. Secure systems dually lead of lower risk and greater uncertainty. In the example context of terrorism and airline security, the aim of

improved security is to reduce the risk of terrorism. Terrorists, Ericson asserts, are in the business of uncertainty and seek to work around new security measures. Hence, the concept of lowering risk through security results in a number of observations:

- 1) The nature of future risks cannot be fully known,
 - 2) Not all risks can be addressed, leaving some unattended,
 - 3) Some uncertainties contain false positives and false negatives,
 - 4) New technologies aimed at reducing risk inherently create new uncertainty,
 - 5) Risk is reactive thus creating new uncertainties,
 - 6) The complexity of risk management can result in unexpected concurrent failures,
 - 7) Catastrophic failures prompt decisions to manage all aspects of the system,
 - 8) Risk managers become increasingly defensive in the face of possible litigation,
 - 9) Excessive statements of risk escalates the amount of system uncertainty,
 - 10) Risk management measures may restrict freedom, invade privacy and discriminate.
- (Ericson 2006).

Together these points raise a number of questions. Can systems be truly secure in the presence of uncertain risk? To what extent does technology improve security versus add additional risk? How much risk is acceptable in these systems? Answering these questions involves both subjective and objective evaluation, making consensus difficult.

In defense of security systems and employees, they aim to protect valuable commodities: the health and welfare of the general public. The difficulty in deploying effective *and* efficient technologies capable of managing an array of risks is a formidable task. Airport security has been compared to the concept of high-reliability organizations. Organizations of this type require nearly error-free operations. One author asserts:

“for commercial air travel to be highly secure, there must be very high levels of technical competence and sustained performance; regular training; structure redundancy; collegial, decentralized authority patterns; processes that reward error discovery and correction; adequate and reliable funding; high mission valence; reliable and timely information; and protection from external interference in operations” (Frederickson and LaPorte 2002, p. 33).

Organizations should then include these internal and external properties if they are to be highly secure. Increasing the money spent on security will undoubtedly provide organizations a number of these tools. However, inherent difficulties in minimizing risk implies money spent to achieve A, B, and C might affect B and C while generating new uncertainties X, Y, and Z.

The means to establish both secure and efficient systems are twofold: people and technology. Indeed, as the next sections will discuss, technology has the ability to improve both security and efficiency. Not without consequence, some argue the idea of advanced security through technology may reduce privacy, a stated liberty of a democratic society. One article details two technologies that may improve security at the expense of privacy. *FaceIt* detects human presence, locates and tracks faces, extracts face images, and performs identification through database matching. The FBI uses *Carnivore* to intercept e-mail communication to combat

terrorism and other felony activities. The author argues that despite proclaiming objective purpose (i.e. improved security), technologies of this type reduce our resistance to privacy (Nelson 2002). The article highlights that even broad social issues, the ideas of privacy and democracy, penetrate the security/efficiency debate.

As mentioned, the debate can be quite heated from all angles. Recent, often intense, criticism of new security measures has only fueled the fire. Often quoted Bruce Schneier describes recent safety measures as a “security theater.” Schneier defines this term as the numerous new security measures that convey safety but accomplish little. He calls government measures since 9/11 “out of proportion to the threat and overly governed by our collective fears” (Kaminsky 2007). The TSA is a common discussion in media. Travelers and advocates have often cited long lines and inconsistent security measures despite significant investment. Bluntly, an apparent joke acronym for TSA among pilots is “Thousand guys Standing Around” (Wilber 2006). Certainly statements of this type are allowed whether or not they are valid and just. Unfortunately, these types of statements can make it difficult for some parties to address the issue objectively.

Research and Case Studies

In light of the issues discussed in the previous section, a reoccurring question looms: can a balance between security and efficiency be defined, achieved, and maintained. Researchers and policy-makers are working towards an answer. This section provides case study pieces to illustrate several failures and successes in defining, achieving, and maintaining the security/efficiency balance.

Case Studies

Screening the Screeners

No matter the side of the security versus efficiency debate, the effectiveness of security measures is a primary concern (only the “bad guys” want ineffective security). However, highly effective security measures are not necessarily more efficient prompting an examination of trade-offs. For example, if it costs \$10 for a system to perfectly secure every \$1 of cargo, you’ve made a bad trade-off and created an inefficient system—despite the fact that the system is highly effective (Kaminsky 2007). However, an ineffective security measure is an inefficient one almost by definition. Therefore, by examining the effectiveness of several aspects of the transportation security system, it may be possible to gain some insight into the effectiveness of the system as a whole.

Since airlines first began conducting passenger/baggage security screenings in an attempt to prevent hijackings, the government has run undercover “tests” to assess the accuracy and efficiency of screeners. These tests usually consist of an individual attempting to bring a prohibited item, undetected, through a security checkpoint. Prior to the formation of the TSA, the Federal Aviation Administration (FAA) tested the baggage screeners employed by various airlines and local companies. As previously mentioned, these tests have revealed a decrease in performance (i.e. banned object detection rate) since 1978. This decline in the performance of checkpoint security is one of the weaknesses that the National Commission on Terrorist Attacks, better known as the 9/11 Commission, pinpointed in its July 2004 report as an area that needs improvement in order to increase the effectiveness of transportation security.

Today the TSA conducts undercover tests of its own screeners. Despite significant increases on security spending and the addition of numerous security employees since 2001, the performance of checkpoint screening continues to decline. In October 2006, the results of Newark International Airport's undercover security screenings were leaked to the press, revealing that screeners had failed 20 of 22 tests, missing multiple guns and explosives (Marsico 2006). Similarly, in July 2007, TSA screeners at Albany International Airport were reported to have failed 5 of 7 security tests (Lyons 2007). What makes this example most notable is that screeners succeeded at identifying and confiscating innocuous recently prohibited items such as bottled water, but failed to identify bomb replicas concealed in the same carry-on bag.

These experiences illustrate some of the key inefficiencies that exist in the current airline security system. The first is that the airport security checkpoint system is organized around a single point of failure (Kaminsky 2007). If a dangerous item/person is not detected while passing through the checkpoint, it is unlikely that they will be detected at all. In cases where a person/item is found to be overlooked at the security checkpoint (a dangerous person/item makes it through the security checkpoint or someone/something enters the concourse without being screened) the only recourse within this system is to evacuate the entire airport and screen again all passengers/packages. This has occurred multiple times at U.S. airports in the last several years for reasons ranging from a late traveler rushing through an unmanned security door at Philadelphia International to the discovery that an unplugged x-ray machine at LAX (Kelley 2002; Stoller 2005). Each of these instances has been an example of security inefficiency; grounding flights for at least two hours and creating delays in air travel that were felt around the country.

The second issue that undercover tests of security checkpoints have illuminated is the difficulty of prioritizing risks. An important part of the debate between transportation security and efficiency revolves around the question of whether transportation funds are better spent training screeners to detect specific security threats (usually based on past specific terrorist plots such as the "shoe bomber") or on emergency preparedness and broader security education. Since attention is a limited resource, every rare but specific threat that security screeners are asked to focus on detracts from their ability to focus on more common risks (Levinson 2006). Coming to an agreement on the appropriate prioritization of risks will be a key step in achieving a satisfactory balance between security and efficiency.

The final issue raised by the failed security checkpoint tests is the debate of whether investing in better technology or a better personnel training is a more efficient use of security funds. Over the last five years a variety of technologies have been developed to remove the "human error" from security screenings and make security more efficient. The Computerized Airline Passenger Screening System (CAPS), which attempts to identify and flag possible terrorists when they check in for a flight, is the most well-known of these systems (Chakrabarti and Strauss 2002). Ideally, a combination of technologies detecting potential terrorists when they check in and enhanced x-ray technology that independently identifies potential explosive devices would prevent security failures like those in Albany. However, technology is expensive and is still not foolproof. Bruce Schneier provides a good example of the security/efficiency issues that exist even with highly accurate technologies:

“Assume an unrealistically optimistic system with a 1-in-100 false positive rate (99% accurate), and a 1-in-1,000 false negative rate (99.9% accurate). That is, while it will mistakenly classify something innocent as a terrorist plot one in a hundred times, it will only miss a real terrorist plot one in a thousand times. Assume one billion possible "plots" to sift through per year, about four per American citizen, and that there is one actual terrorist plot per year. Even this unrealistically accurate system will generate 10 million false alarms for every real terrorist plot it uncovers. Every day of every year, the police will have to investigate 270,000 potential plots in order to find the one real terrorist plot per month” (Schneier 2007).

As a result, investing in greater training for security personnel may be a more efficient approach.

El Al: Israel’s Approach to Airline Security

This report has presented a theoretical approach to analyzing security/efficiency trade-offs (Johnston 2004) and has discussed several debates over best practices to achieve a security/efficiency balance within the American airline industry. Examining the policies of another country is an exercise that can help inform debate and policy change, especially with overly politicized issues such as security. An interesting case study to examine on this topic is El Al Airlines, the largest airline in Israel and also reputed to be the most secure airline in the world. El Al’s approach to balancing airline security and efficiency is an interesting example because the historic political unrest in Israel necessitated that the airline place a high value on security and preventing terrorism from its beginnings.

Like the TSA, El Al’s security measures have been subject to some criticism. It is the Israeli government and El Al’s broader approach to security that makes it an interesting case study. El Al has a security budget of roughly \$80 million, covering Ben Gurion International Airport near Tel Aviv and the airliners themselves (Tucker 2003). With this budget the airline, with the assistance of the Israeli Security Agency, Shin Bet, provides several levels of security spanning from the exterior of the airport to the planes in the air. Armed guards examine cars on the single access road leading into Ben Gurion airport and plainclothes security officers monitor the terminal for suspicious activity and regularly check different areas (i.e. trash cans, etc.) for explosive devices (Tucker 2003). All El Al aircraft are equipped with double reinforced cockpit doors and are flown by pilots with hand to hand combat training. An armed plainclothes sky marshal is a passenger on each El Al flight and all aircraft have steel reinforcements to protect the aircraft and passengers from an explosion in the cargo bay (Schuman 2001).

Beyond this multi-layered approach to security, the main factor that differentiates the Israeli approach to security is its emphasis on psychological profiling and human factors as opposed to simply screening baggage (Tucker 2003). All El Al passengers are interviewed briefly before boarding the aircraft and observed for suspicious behavior and body language (Schuman 2001). The reason for this alternative approach is because explosives and other devices used by terrorists can be so creatively and well concealed that it would be virtually impossible to identify and discover them in luggage. Screeners who are well-trained in psychological profiling, on the other hand, should be able to pick up on body language and other clues during questioning that indicate whether or not a person poses a threat.

El Al also relies on several forms of sophisticated technology as a back-up to their human-centered approach to security. For example, all baggage is passed through a chamber that simulates the low pressure environment of a plane in flight that may trigger some explosives (Simcoe 2007). El Al is the only commercial airline to use this technology. Luggage is also screened using more traditional methods and is sometimes checked by hand. El Al security staff are responsible for checking the baggage on their flights, even at airports in other countries that are run by other agencies (Tucker 2003).

While the El Al approach to security is still vulnerable to problems of human error and other flaws, this unique approach can be used to inform US transportation security policy. The El Al example introduces several new security/efficiency trade-off questions, but can inform several of the debates discussed in the previous case study. For example, El Al presents a model to address the inefficiencies of a security system with a single point of failure.

Policy

Non-Airline Policies

Although scholars and intelligence experts warned policymakers about the threat terrorism could present to the transportation system before the attacks of September 11th, the United States approach to transportation security continues to be reactive as opposed to directive. A prime example of reactive security is the TSA's overwhelming focus on commercial passenger air travel. As mentioned previously, the TSA is the federal agency responsible for securing *all* modes of transportation, including highways, railroads, maritime, and non-passenger air travel. Relative to pre-9/11 levels, funding for transportation security has increased significantly since the deployment of TSA as has the number of transportation security employees. The TSA budget increased by \$3.5 billion between 2002 and 2003 alone and the number of security screeners employed peaked in 2003 at nearly 60,000 (United States Department of Transportation 2003; Peterson 2007).

Due to several extreme past events, the majority of these screeners and the TSA's budget is dedicated to one segment of a single mode—commercial passenger air travel. In fiscal year 2006, \$4.6 billion of the \$5.7 billion in TSA funding approved by the House was to be dedicated to commercial aviation security (Wodele 2005). After accounting for this spending, \$1.1 billion remains to secure other modes of transportation and the 97% of landing facilities that do not house commercial airlines (Williams 2007).

As a result, little has changed in the area of non-airline security policy over the last 6 years. For example, of the approximately 17,000 cargo containers that the United States receives each day, only about 2% are physically inspected (Closs and McGarrell 2004). Despite the fact that non-airline modes have been the subject of terrorist plots and events such as the theft of a cyanide truck in 2002 have posed serious risks to public safety and security, these modes have not been subject to the same “knee jerk” policy response that has driven airline security policy over the last 5 years (Closs and McGarrell 2004; DeLorenzo and Murray 2004). This may be because the businesses that depend upon cargo transportation and other modes place a higher value on efficiency, therefore requiring more innovative new policy approaches. For example, as opposed

to simply increasing the number of freight inspections, which would require a vast amount of time and resources, the Container Security Initiative led by the Customs Department emphasizes risk assessment and moves inspection earlier in the supply chain to maximize efficiency (Closs and McGarrell 2004). This approach may provide an alternative policy model for commercial air travel in the future. However, it should be noted that bills have recently been passed in both the House and Senate that would require 100% inspection of all cargo transported on passenger airlines to be inspected with the same type of x-ray machine used at baggage screenings. This legislation could have large implications for the security/efficiency balance in cargo transportation (Office of Inspector General 2007).

Airline Policies and Recommendations

This report has discussed in detail the role of the TSA. Long lines and seemingly silly policies (removing belts) frustrate passengers. Security remains important, however, and many challenges exist to improve the effectiveness of searches as well as ensuring that the burdens of effectiveness are proportional to the risks and costs. This section will address some recommendations to improve security procedures and efficiency, including the Computer-Assisted Passenger Screening System (CAPSS) program, and general screening of cargo on passenger airlines. Again, trade-offs exist between changing, adding or eliminating procedures to improve security or efficiency.

A number of intriguing recommendations were proposed by researchers at the Massachusetts Institute after creating an algorithm to defeat the CAPS system. The pair of researchers termed it the “carnival booth”. Similar to “security theater”, the name references a carnie inviting a terrorist to try their luck. The researchers found the CAPS system was error prone and easy to defeat. Terrorists can too easily determine if they have been flagged and use that knowledge to their advantage (Chakrabarti and Strauss 2002). The author’s suggest flagging be non-obvious.

The first of these recommendations calls for improved object screening through technology (e.g., x-ray). This technique has been evolving for several years. In August of this year the TSA began testing new x-ray machines at three airports and could buy as many as 500 this fall for deployment at commercial airports. The new machines are more effective at screening bombs and could improve efficiency by allowing different luggage angles on a single pass. (Frank 2007).

The authors next recommend merging passenger x-ray technology and standard metal detectors into one device. Similar to many recommendations, this one seems to be less apparent to policy-makers who call for things like more employees, resources, training, and better self-audits. Such a recommendation reduces the carnival booth effect. Instead of removing people from the line and scanning those identified as potential risks, a security office could discretely use the more costly x-ray scanner on passengers deemed as ‘flight risks.’

Their last recommendation seems to finally fall in line with the broader ideas of policy makers and bureaucrats. The authors suggest better-trained security employees, varied questioning, and improved screening will be the most effective deterrents. While applying identical security policies to all passengers sounds great to those motivated entirely by improved security, it would likely be a monumental loss to efficiency in airline travel. If some of the above

recommendations were implemented, it is possible that airport security might move just a little bit closer to the appropriate balance.

The Government Accountability Office published a report in May of 2005 that analyzed the quality of the training and performance of passenger screeners. The reports findings can be mostly summed up by the following: “TSA lacks adequate internal controls to provide reasonable assurance that screeners receive legislatively mandated basic and remedial training, and to monitor its recurrent training program” (United States Government Accountability Office 2005, pg. 2). As a result of these findings, the GAO recommended several new policies regarding screener training and oversight.

One concern is the lack of internet/intranet connectivity among TSA training facilities. The GAO recommends TSA develop a strategy to deploy high-speed internet/intranet connectivity to improve screener training. The GAO also recommended that the TSA develop internal control that define responsibilities for monitoring and documenting the completion of required training”

A recent Homeland Security report focused on improvements needed for improved security, with only nominal regard for efficiency. The report indicates that TSA “does not provide sufficient resources for air carrier inspection coverage. Therefore, Aviation Security Inspectors do not have the capability to monitor cargo screening activities and are unable to report accurately on air carrier compliance” (Office of Inspector General 2007, pg. 1). Procedures and practices with regard to passenger aircraft cargo seem fraught with inconsistencies, noncompliance and lack of policies to comply with. Echoes of the GAO’s assessment of passenger screening resonate through DHS’s assessment of cargo screening.

The report concludes with two major recommendations, each with more specific actions within them. The first is a broadly reaching recommendation aiming to establish a system of procedures for cargo screening and inspection with several elements. Those elements include clearly written training guidance and training, procedures to improve inspections, guidance on security program requirements, a quality control program, and providing sufficient resources to the cargo inspection program (Office of Inspector General 2007).

The second concerns the Performance and Results Information System (PARIS) that is the primary management tool for monitoring the quality and quantity of inspections” (Office of Inspector General 2007). DHS recommends that the TSA improve PASIS by providing better guidance, detailed training, and greater funding. The TSA agrees with these recommendations, however all but one “will remain open because, in most cases, the actions that TSA indicates the agency has taken or will take, do not fully address [DHS] concerns and corresponding recommendations” (Office of Inspector General 2007).

A potentially disturbing addendum to the recently passed law requiring inspection of all cargo transported on passenger airlines was reported recently. “The TSA says it is interpreting the statute to allow boxes sealed by government-certified shippers to be loaded directly on planes. TSA spokesman Christopher White said freight ‘is inherently screened’ if it is packed with tamper-evident seals at a facility that meets federal security standards” (Savage 2007). Indeed, the idea of creating further uncertainty through such measures seems likely.

Conclusion

The balance of security and efficiency in the context of transportation in the U.S has yet to be achieved. The creation and evolution of the current transportation security system has been a reactive process. Historical security systems leaned toward efficiency. September 11 and a number of successive events swung systems toward security, prompting significant funding with the aim of improving security. The focus of the expenditures has been airline security as the federal government spends 80 percent of a 5.7 billion dollar transportation security budget on commercial airline travel. Owing to a single point of failure, the current security system at airports has been proven to be ineffective and inherently inefficient. A number of factors might explain these findings. The first is the difficulty in determining whether to invest in people or technology. The second is whether to invest on preventing rage specific attacks, such as 9/11, or in general emergency preparedness.

The government response to these points is vague. Some claim the backups and so called “security theater” represent worthwhile trade-offs in terms of efficiency and civil liberties. Critics cite poor statistics and examples in other countries such as England and Germany, where officials seem to be stopping terrorist plots before the airport using police investigation. TSA’s then typical response is to boost baggage checks. Dozens of other recommendations exist but, attributed to the factors discussed within, solutions are not easy.

It is difficult to determine whether security is the enemy of efficiency. In an ideal system, where a more complete evaluation of tradeoffs is possible, this statement might be false. Well trained security personnel and advanced technology could allow for effective, efficient systems. The evidence presented, however, seems to suggest today’s security systems, especially in the airline industry, are both ineffective and inefficient.

Transportation systems have a life cycle of discovery, growth, and maturity. Air transportation in itself is a mature system. Prior to 9/11, people might have argued airline security was also mature. Since then, new questions and threats have emerged challenging the maturity of airline security. Perhaps airline security is actually in the growth phase, waiting for new procedures and technologies to advance the system and achieve a balance point between security and efficiency.

An examination of this type raises a number of points for discussion:

- 1) Is security the enemy of efficiency?
- 2) How can we weight security concerns against efficiency needs?
- 3) Are we making good or bad security tradeoffs? Efficiency tradeoffs?
- 4) Is it possible to develop decision and/or performance criteria to define, achieve, and maintain a balance between security and efficiency?
- 5) What are your thoughts on the terms “security theater” and “carnival booth”? Can security theater help increase efficiency tradeoffs? Do these terms only add fuel to the fire?
- 6) Is a life-cycle approach a useful or practical way to describe policy?
- 7) Can systems be truly secure in the presence of uncertain risk?

- 8) To what extent does technology improve security versus add additional risk?
- 9) How much risk is acceptable?

Establishing a dialogue to answer questions of this type is useful and necessary among and between legislators, regulators, and the regulated.

References

- Chakrabarti, S. and A. Strauss. (2002). "Carnival Booth: An Algorithm for Defeating the Computer-Assisted Passenger Screening System." MIT Project on Mathematics and Computer Retrieved September 6, 2007 from <http://www.swiss.ai.mit.edu/6805/student-papers/spring02-papers/caps.htm>
- Closs, D. J. and E. F. McGarrell (2004). Enhancing Security Throughout the Supply Chain, IBM Center for The Business of Government.
- DeLorenzo, J. and D. Murray (2004). National Safety & Security Field Operational Test: Technologies to Improve Security and Efficiency in the Hazardous Materials Transport Industry. Security Technology, 2004, 38th Annual 2004 International Carnahan Conference.
- Ericson, R. V. (2006). "Ten Uncertainties of Risk-Management Approaches to Security." Canadian Journal of Criminology and Criminal Justice **48**(3): 345-356.
- Frank, T. (2007). "New X-ray machines could speed security." USA Today Retrieved September 13, 2007 from http://www.usatoday.com/news/nation/2007-08-30-xray_N.htm.
- Frederickson, H. G. and T. R. LaPorte (2002). "Airport Security, High Reliability, and the Problem of Rationality." Public Administration Review **62**(s1): 33-43.
- International Air Transport Association (2006). "The Air Transport Industry Since 11 September 2001." Retrieved September 13, 2007, from <http://www.iata.org/NR/rdonlyres/92FC0755-1D63-4931-A983-847CC1EA897A/0/airtransportsince911.pdf>
- Johnston, V. R. (2004). "Terrorism and Transportation Policy and Administration: Balancing the Model and Equations for Optimal Security." Review of Policy Research **21**(3): 263-274.
- Johnston, V. R. and A. Nath (2004). "Introduction: Terrorism and Transportation Security." Review of Policy Research **21**(3): 255-261.
- Kaminsky, J. (2007). "Everything We Know About Security is Wrong." Citypages Retrieved September 6, 2007, from <http://citypages.com/databank/28/1394/article15776.asp>.
- Kelley, T. (2002). "Briefly Noted; Airport Evacuation." The New York Times Retrieved September 7, 2007 from <http://query.nytimes.com/gst/fullpage.html?res=980DE2DA113EF930A15751C0A9649C8B63>.
- Khalid, N. (2006). "Too Much of a Good Thing? Some Reflections on Increased Security and its Costs." Defense & Security Analysis **22**(3): 261-273.
- Levinson, D. (2006). "Security is the enemy of efficiency, or attention is a scarce resource." The Transportationist a weblog by David Levinson at the Nexus of Networks, Economics, and Urban Systems Retrieved September 6, 2007 from http://blog.lib.umn.edu/levin031/transportationist/2006/12/security_is_the_enemy_of_effic.html
- Lyons, B. (2007) "Fake bomb eludes airport test." Times Union Retrieved September 7, 2007 from <http://timesunion.com/AspStories/story.asp?storyID=603177&category=REGIONOTHER&BCCode=&newsdate=7/9/2007>.
- Marsico, R. (2006). "Screeners at Newark fail to find 'weapons'" Star Ledger Retrieved September 7, 2007 from <http://www.nj.com/news/ledger/index.ssf?/base/news-9/1161928940141470.xml&coll=1>.
- Nelson, L. (2002). "Protecting the Common Good: Technology, Objectivity, and Privacy." Public Administration Review **62**(s1): 69-73.

- Office of Inspector General (2007). Transportation Security Administration's Oversight of Passenger Aircraft Cargo Security Faces Significant Challenges (Redacted). U.S. Department of Homeland Security.
- Peterson, B. S. (2007). "Inside Job: My Life as an Airport Screener." CondeNast Traveler Retrieved September 13, 2007 from <http://www.concierge.com/cntraveler/articles/detail?articleId=10624&pageNumber=3>
- Savage, C. (2007) "No checks for bombs in certified air cargo." Boston Globe Retrieved September 13, 2007 from http://www.boston.com/news/nation/washington/articles/2007/08/24/no_checks_for_bombs_in_certified_air_cargo/
- Simcoe (2007). "El Al Decompression Chamber." Simcoe Engineering Group Limited Consulting Limited Retrieved September 12, 2007 from <http://www.segl.com/xj.php>
- Schneier, B. (2007). "How to Not Catch Terrorists." Appeared in the March 26, 2007 issue of Forbes Retrieved September 10, 2007 from <http://www.schneier.com/essay-163.html>
- Schuman, E. (2001). "El Al's legendary security measures set industry standards." Israel Insider Retrieved September 12, 2007 from http://www.israelinsider.com/channels/security/articles/sec_0108.htm
- Stoller, G. (2005). "Mounting evacuations add to fliers' list of frustrations." USA Today Retrieved September 7, 2007 from http://www.usatoday.com/money/biztravel/2005-05-10-evacuations-usat_x.htm
- Tucker, J. (2003). "Strategies for Countering Terrorism: Lessons from the Israeli Experience." Retrieved September 12, 2007 from <http://www.homelandsecurity.org/journal/articles/tucker-israel.html>
- United States Department of Transportation. (2003). "U.S. Department of Transportation 2003 Budget in Brief Transportation Security Administration." Retrieved September 13, 2007 from <http://www.dot.gov/bib2003/tsa.html>
- United States Government Accountability Office (2005). Aviation Security: Screener Training and Performance Measurement Strengthened, but More Work Remains.
- Wilber, D. Q. (2006). "TSA Tries to Balance Security, Efficiency." The Washington Post Retrieved September 7, 2007, from <http://www.washingtonpost.com/wp-dyn/content/article/2006/08/13/AR2006081300391.html?referrer=emailarticle>.
- Williams, C. (2007). General Aviation Safety and Security Practices: A Synthesis of Airport Practice. Airport Cooperative Research Program, Transportation Research Board.
- Wodele, G. (2005). "Bush administration's TSA budget request faces steep cuts." Retrieved September 12, 2007 from <http://www.govexec.com/dailyfed/0805/081005tdpm1.htm>.