AIRPORT SECURITY: CURRENT PRACTICE AND PERSPECTIVES FOR 2030

Samson Fatokun[a]

Embry-Riddle Aeronautical University, Daytona Beach, Florida, USA

ABSTRACT

The high profile of aviation has made it an attractive target to terrorist activities. The September 11 terrorist attack and subsequent failed terrorist attacks made safety and security top priorities for the aviation industry. A review of the current practice in airport security conducted by the author found that it was reactive, expensive and inefficient in some areas based on a "one-size-fits-all" principle. The forecast of a new approach to airport security conducted in this study predicted that by 2020-2030 airport security will be proactive and based on passenger differentiation.

Keywords: Airport security, risk-based approach, scenario-based approach, passenger, differentiation, proactive.

[a] Samson Fatokun is a Ph.D. in Aviation candidate at Embry-Riddle Aeronautical University, Daytona Beach, Florida, USA. Samson lives in Lagos, Nigeria.

1. INTRODUCTION

Since September 11, 2001, airport security has taken new dimensions throughout the world. Airport security has become a regular part of the passenger travel experience as a lot of attention is being paid to different ways the processes and procedures can be made more efficient and effective. In spite of improved measures introduced for airport screening and for the accurate identification of people whether they happen to be airport staff, passengers or contractors on airport sites, there have been several attempted terrorist attacks on commercial flights since September 11.

In December 2001, Richard Reid on board an American Airlines flight from Paris to Miami attempted to ignite an explosive device hidden in his shoe. Also in 2008, a Somali woman attempted to hijack an Air New Zealand flight and most recently a Nigerian national named Umar Farouk Abdulmutallab on December 25 2009 attempted to detonate an explosive device in his trousers while on board a Delta flight from Amsterdam to Detroit (Holbrook, 2010). How did all these dangerous individuals come so close to achieving their terrorist objectives when airport security was greatly improved after September 11, 2001 (Holbrook, 2010)?

In addition to those setbacks, the operation of the present airport security system has put the burden of space, layout, training of staff, technology and inflexibility of processes on airport operators. Passengers have also been dealing with long security lines, complexity of rules and often invasive processes (IATA, 2013). The need to modernize and improve passenger security screening at airports has become a topic of discussion across the aviation industry. The paper will review the current practices in airport security; consider some new approaches that are emerging in the industry and attempt to forecast an approach to airport security for the 2020-2030 timeframe.

2. PURPOSE OF THE STUDY

There have been several developments in recent years related to more efficient airport security such as the implementation of machine readable passport, introduction of more sophisticated scanners at checkpoints and addition of new items on the list of items banned in bags permitted in the cabin. In spite of these developments, threats to aviation security still remain, thus the constant search for more efficiency in airport security. The intent of this research is to forecast the approach in 2030 taking into consideration current practices and emerging trends in airport security.

3. SCOPE OF THE STUDY

This study will not consider aviation security as a whole but will focus on aviation security at the airport level only. Airport security is an important component of aviation security. In considering airport security, the focus of this study will only cover passenger security at the airport, baggage and cargo screening.

4. IMPORTANCE OF THE STUDY

According to Napolitano, the former United States Secretary of Homeland Security, aviation security tops the priority list of the Department of Home Security (Peters, 2010). Safety and security continue to be on the priority list of the aviation industry. Moreover, the combination of the predicted growth in air travel and the continuously evolving security threats makes it important that the current approach to airport security be reviewed and we forecast a future approach to airport security that will secure the expected growth in air travel.

5. LITERATURE REVIEW

The introduction of biometrics at airport checkpoints was greeted with great hope. Houdeau (2009) considered biometric identification as a necessary check for travel documents, border control and immigration. Houdeau argued that three biometric technologies have emerged: (1) face recognition applied in areas such as e-passport, (2) fingerprint recognition applied for Schengen visa and (3) iris recognition.

One of the challenges facing airport managers is the ability to accurately identify people in the airport environment, whether they are passengers, staff or contractual workers who need to work on-site at the airport. Airport security needs a tool that will help determine who and then certify all who need to have access to critical airport areas. Elliot (2009) while analyzing the importance of biometrics for airport security argued that biometrics could be useful mostly to mitigate the limitations of personal identification number (PIN) access. He believed that the use of face recognition technology was a compelling solution offered by biometrics when compared to a PIN that could be lost or stolen. Elliot (2009) presented other biometrics such as finger-prints, iris and palm.

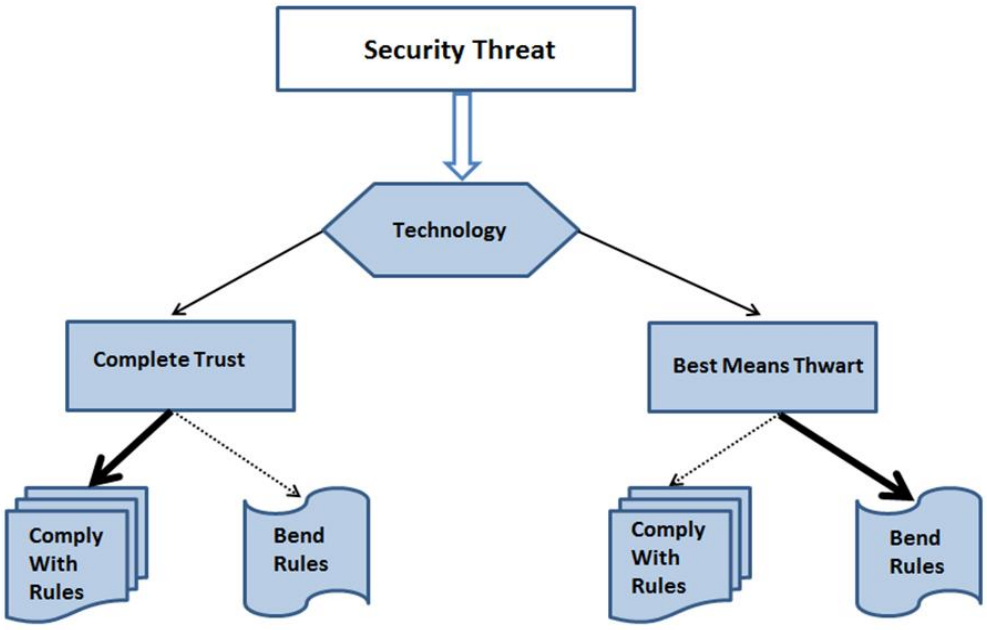
Moreover, reactions to the September 11, 2001 terrorist attacks renewed further attention to biometrics. However, Gold (2012) analyzed the performance of the biometrically-enabled e-gates which were expected to speed up immigration checks at London Heathrow Airport and found that they actually slowed the passengers down, even when the e-gates systems were

set to allow false positive. It was found that the facial recognition system at the e-gates lost its sensitivity to the point that a woman could pass through the gate using her husband's passport by accident (Gold, 2012).

The challenges presently encountered in airport security are not limited to biometrics. IATA (2013) in its review of the present state of airport security found that there was no connectivity and networking within the airport checkpoints and with other systems at airports. This has been resulting in airports systems acting independently. The situation has also reduced their ability to provide real time data that can enhance passenger screening at airport checkpoints. At many airports, there is neither communication nor coordination between the immigration checkpoints and the passenger and cabin baggage checkpoints.
Kirschenbaum, Mariani, Gulijk, Rapaport & Lubasz (2012) considered the issue of the technological adequacy at airport checkpoints from the human and technology perspectives. They conducted a field survey of airport employees spread over eight airports in Europe to analyze the relationship between the trust in security technology and the implementation of security rules and regulations at airports. To guide their research Kirschenbaum et al (2012) posited a theoretical working model (Figure 1 below) that considered trusting technology as a two-pronged construct consisting in complete trust in security technology devise and a means of obtaining a security decision. The employee's trust in either of the two views could have an impact on the level of compliance with security rules and protocol.

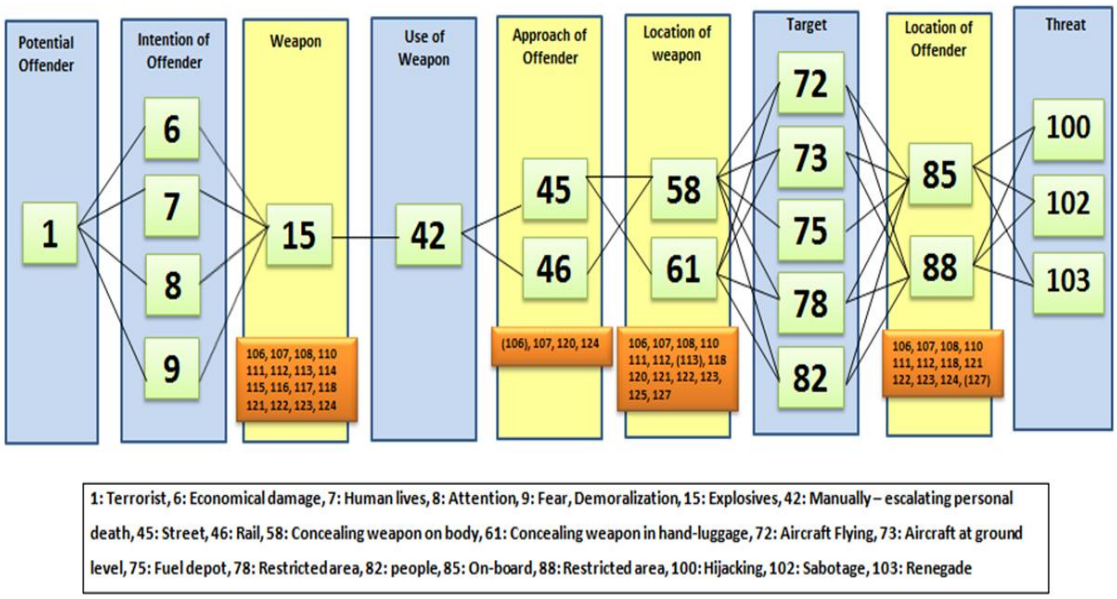
The study found that employees who completely trusted security technology tended to follow the rules. Those who consider security technology as a best means of catching offenders tended to bend or break the rules if the situation called for it (Kirschenbaum et al, 2012). The above technological setbacks and the human factor challenges in aviation security are driving research for a new approach to airport security. Cole & Kuhlmann (2012) advocated for a scenario-based approach to airport security. Having observed that so far aviation security has been reactionary to threats, they researched the application of enhanced scenario-planning methods to airport security to make it proactive. Their approach has the merit of determining threat scenario clusters. The analysis of those scenarios could help airport security operatives: (1) better anticipate possible future threats, (2) identify weak points in the security architecture for improvement and (3) put in place effective security measures to counter threats before they manifest. Through figure 2 below, Cole & Kuhlmann (2012) illustrated how some threat scenarios can be opposed to security counter-actions and be exposed.

Figure 1 - Theoretical working model of security decision making tree linking technology and compliance to security rules



Source: Kirschenbaum et al (2012)

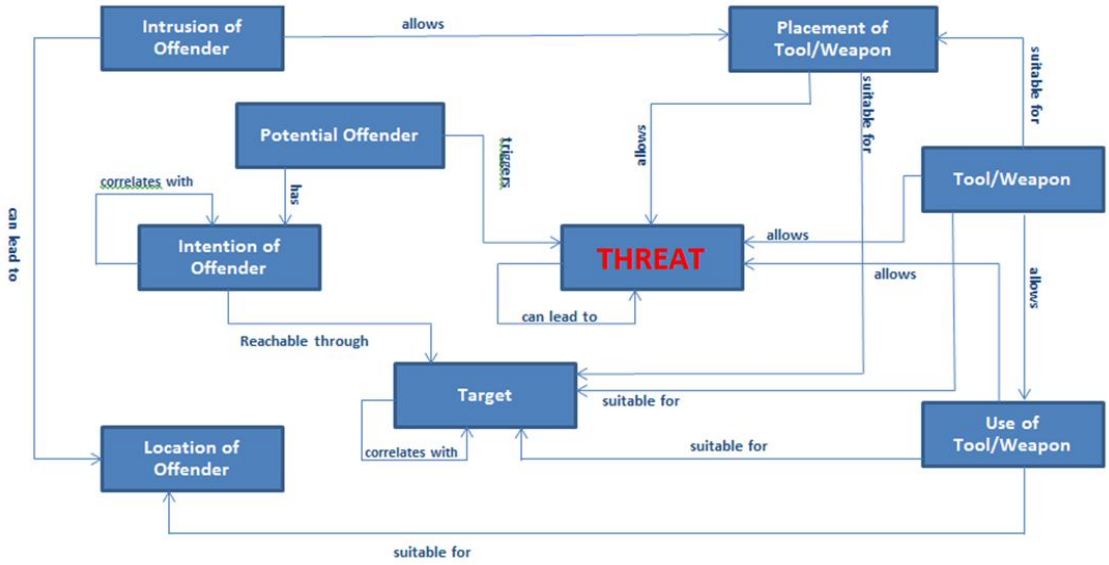
Figure 2 - Threat Scenario Cluster with respective Security Measures



Source: Cole & Kuhlmann (2012)

In the flow chart of figure 3 below, the authors looked at some domains that constituted scenarios and how they were interlinked. The arrows in the flow chart represent not only the direction but also the quality of the relation between two domains. Threat scenarios are built from the relations between the domains. The work of Cole & Kuhlmann (2012) is channeling a course for airport security in the future. It is a departure from the present reactionary and "one-size-fits-all" approach that relied mostly on technological improvement and moving to a scenario-based proactive approach.

Figure 3 - Details of flowchart (showing 9 out of 15 domains)



Source: Cole & Kuhlmann (2012)

6. RESEARCH DESIGN

Further to the literature review (important for this research), the author reviewed past and present approaches to airport security in order to determine their strengths and weaknesses. The research then proceeded with a forecast for airport security in the 2030 time frame. As the subject involves a review of past and current practices in airport security, the researcher made use of documents and other archival materials. The author used the archival design to achieve his research objectives. Vogt, Gardner & Haeffele (2012) recommended the use of an archival design when the subject involves the past or when the materials are not currently available. Articles from peer-reviewed journals were the primary source of literature for this study. While not extensive, the researcher found some articles related to airport security that have been published by peer-reviewed journals. Also, important policy

documents for the aviation industry such as Annex 17 of ICAO that relates to aviation security were also consulted extensively.

7. ANALYSIS

7.1 Current Practices in Airport Security

A) National Standards

Annex 17 of ICAO provides some broad standards and recommended practices (SARPs) for the handling of aviation security. Those recommended practices have been adopted by many countries and integrated in their national standards. Even though some commonalities can be observed in the operation of airport security, the practice of airport security is based on national standards and regulations. Therefore, the practice of airport security is not uniform worldwide. This explains why a passenger may be required to observe a security measure in one country and not be required to observe the same measure in another.

In the European Union (EU), the Commission Regulation (EU) 185/2010 set forth the measures for the implementation of the common basic standards for aviation security. In the United Kingdom (UK), the Department for Transport (DFT) is responsible for airport security. The UK has been contemplating the use of new methods of passenger screening for more efficiency. In India, due to the location of slums close to some airports, passengers can be required to undergo additional searching of hand luggage. In Israel, passengers leaving the country are checked against a computerized list maintained by the Israeli Ministry of Interior (Wikipedia, 2013). Airport security standards are not globally harmonised.

B) Operations of Airport Security

The current practice in passenger screening at airports has consisted of making all departing passengers go through a minimum of two checkpoints. The first checkpoint is the border control where often biometrics are used to authenticate travel documents which ensures that the bearer of the travel document is the person described in the travel document and ascertains that the passenger has the required documentation to cross over the border. Biometrics technology such as iris recognition, fingerprint recognition and face recognition are used by border control agents to achieve their purpose of identification, verification and authentication. Some countries support the biometrics with security intelligence information stored in border control systems. Biometrics have helped to curb the use of impersonation and fake documentation. The matching of the finger prints on the travel document is now

compared with those collected from the traveler at immigration checkpoints when entering the country to help reveal impersonation.

However, as highlighted in the literature review, biometric technology has shown its limitations for example the failure of face recognition technology which allowed a woman traveling with her husband passport to pass through an e-gate in London (Gold, 2012). Building redundancies and constant improvement in biometric technology, supported with strong passenger intelligence data, will help to improve the efficiency of border control checkpoint. The efficiency of border control checkpoints also hinges on reducing long queues at immigration checkpoints.

Passenger and cabin baggage screening point is another checkpoint that all passengers are required to go through before proceeding to board their flights. Typically, at this checkpoint, all passengers are requested to walk through a metal detector or a body scanner machine. Passengers who trigger the alarm of the metal detector machine or body scanner are taken through a secondary check that may involve a pat down. At times passengers are also randomly selected for a secondary screening. In some less developed countries where airport security infrastructure is adjudged minimal or average, airlines take it upon themselves to conduct a secondary passenger and cabin baggage screening before boarding in order to protect their flights. This practice of secondary screening has been a source of additional cost for airlines and an additional hurdle for passengers.

While the passenger is walking through the metal detector, cabin baggage is taken through a separate x-rate device. According to national standards, the cabin baggage control may require screening of coats, jackets, belts, shoes, laptops, gels, liquids and aerosols. At prominent airports and at times randomly, explosive trace detection devices are used to screen cabin baggage.

After the Lockerbie bombing, screening of check-in baggage that is loaded into the hold of aircraft was introduced in the standards and recommended practices of Annex 17 of ICAO. The Annex 17 recommends 100% screening of hold baggage for the detection of explosives. The practice of loading only the baggage of passengers who have boarded the aircraft became a standard for the dispatch of commercial flights. Airlines have been practicing passenger and baggage reconciliation. This practice explains the fact that flights do not depart until the loaded baggage of a passenger who misses his/her flight is off-loaded.

From the above we can observe that the current operation of airport security is characterized by long queues and redundancies. A passenger with many connections can be screened three or four times on any particular journey if they leave the airports secure area. The passenger may be screened at every airport where he/she makes a connection. Also there is lack of connectivity between the checkpoints. For example, at many airports, there is no live exchange of information between the airline check-in desk, the immigration checkpoint, and the airport security checkpoint.

C) Present Reactionary Approach to Airport Security

The present approach to airport security has been highly reactive. It lacks in proactive qualities. The screening of passenger shoes at checkpoints was not introduced until a passenger concealed explosive device in his shoes. Similarly, the screening of liquid was not instituted until a passenger attempted to use some liquid substances for explosive purposes. The scenario applies to the Christmas Day bomber who was able to pass through many security checkpoints through many countries without the explosive concealed in his trousers being detected. Full body scanning was not introduced until after the failed attempt. Thus, the threats have been ahead of security measures. Therefore one can argue that the present airport security approach has only been reacting after damage has been done or after a failed attempt or a near miss. Airport security must move from a reactive approach to one that is proactive.

D) Airport Security Funding

Airport security in its present form is expensive. It was reported that the American TSA employed about 50,000-person workforce in 2010, those employees screened an average of 2 million travelers a day across 457 airports (Ott, 2010). This puts a heavy financial burden not only on the state but also on the airlines and passengers. Airlines spend approximately $8.55 billion per year on security related costs (IATA, 2013).

In countries where airlines have to provide secondary screening to secure their assets, they bear the burden of additional cost in a business that is marginally profitable. Some governments introduced security taxes and charges to fund airport security expenses. Those security taxes are collected through additional passenger charges on the flight tickets. These charges lead to an increased airfare which, in turn, negatively impact demand for air travel (Vasigh, Fleming & Tacker, 2008). The aviation industry needs to find an efficient and cost-

effective approach to airport security that will mitigate the negative impact of airport security charges on the demand for air travel.

7.2 Trends and Future Perspectives for Airport Security

From the above review, one can arguably state that the present airport security is reactionary, expensive, based on a uniform approach and lacks efficiency in some areas. The new approach to airport security attempts to mitigate those setbacks. If a new approach to airport security is to find acceptance in the aviation industry, it has to be proactive, more efficient and less expensive than the current approach.

A) Scenario-Based Airport Security

The scenario-based approach to airport security proposed by Cole & Kuhlmann (2012) is certainly a step in the right direction and departs from the reactionary approach. Using a scenario-based approach, airport security managers will be able to generate clusters of possible scenarios of threats to airport security that will give them the opportunity to proactively devise measures to counter those threats before they are carried out. Threat scenarios will also help airport security managers review the existing airport security architecture and thus help to detect areas of weakness. Moreover, the scenario-based approach departs from the uniform approach that applies the same level of screening to all passengers. With the scenario-based approach, airport security rules will not apply to all passengers the same way and will depend on the outcome of played out scenarios. This fulfills some expectations of the new approach to airport security as stated above.

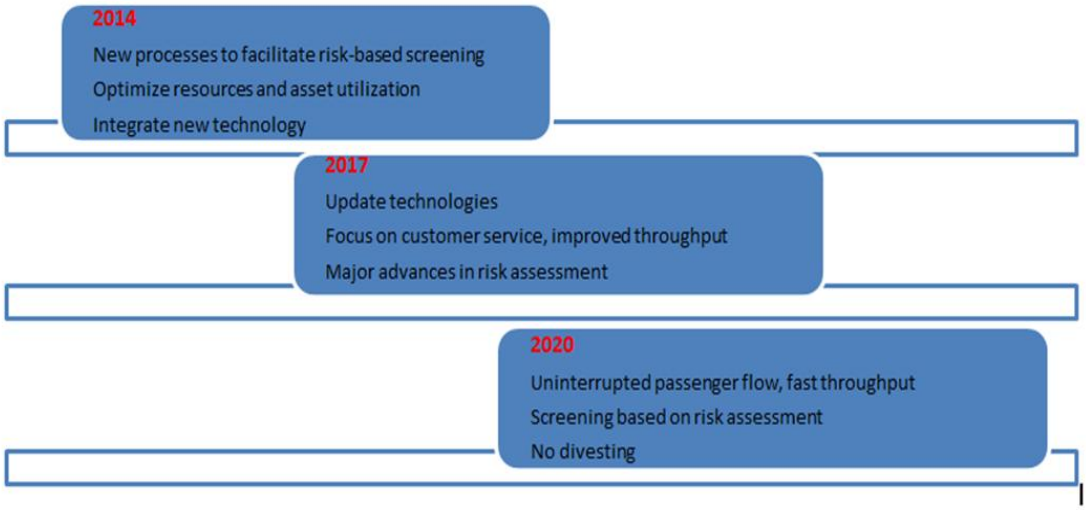
However, the challenge of this approach is the lack of certainty that all possible scenarios have been captured by the system at any given time. The reliance on literature and airport security experts for the generation of domains that will form into scenarios may not be sustainable. As in aviation safety, a scenario-based approach will need a voluntary reporting system that will be a reservoir of domains that can be used to make complete scenarios.

B) The IATA Checkpoint of the Future: A Risk-Based Approach

The International Air Transport Association (IATA) having found that the current approach to airport security is not sustainable due to the projected future growth in air travel, has been advocating for a “Checkpoint of the future” that is a risk-based approach focused on: (1) strengthening security, (2) increasing operational efficiency and (3) improving the passenger experience (IATA, 2013).

IATA believes that threats to aviation security are generated by a very few number of travelers. The great majority of passengers are of no threat to aviation security. It is therefore not necessary to subject all the passengers to the same level of screening at airport checkpoints. Thus, its advocacy for a risk-based passenger differentiation whereby air travelers are screened differently according to their levels of risk (IATA, 2013). The risk assessment process cannot be based on religion, race or gender but it will be based on travel data, intelligence gathering, voluntarily contributed information and behavior detection technique. It will be a continuous process that spans from reservation to boarding (IATA, 2013). IATA proposed a phased approach which will result in uninterrupted passenger flow and fast throughput by 2020 as shown in figure 4 below.

Figure 4 - IATA phased approach risk-based aviation security



Source: IATA (2013)

7.3 Complementarity of the Scenario-Based Approach and the Risk-Based Approach

IATA's "Check Point of the Future" is a risk-based approach geared toward passenger facilitation at airports with one of its major outcomes being passenger differentiation which consists of screening passengers based on their category's profile, thereby leading to improved efficiency and security at airports. The risk assessment component of IATA' s "Check Point of the Future" requires a more robust approach than the current approach based on passenger data, behavior analysis and identity management to gain the trust of national regulatory authorities. It needs to be based on a proactive process that is able to identify not only historic threats but also future threats. This anticipatory process is provided by the scenario-based approach of Cole & Kuhlmann (2012).

Risk is defined by the following equation where R stands for risk, S for severity and L for likelihood: Risk equals severity x likelihood (Stolzer, Halford & Goglia, 2008).

$$R = S \times L \quad (1)$$

The likelihood element in the risk assessment of the "Check Point of the Future" is provided by the scenario-based approach of Cole & Kuhlmann (2012) which follows the process of; (a) environmental scanning, (b) selection of threat elements, (c) reduction of connections, (d) cross-impact analysis and (e) scenario building.

On the other hand, a scenario-based approach to airport security is incomplete if it does not ultimately lead to improved passenger facilitation at airport checkpoints as advocated by IATA's "Check Point of the Future". Therefore, it is recommended that the airport security perspective for 2030 should include an integration of the scenario-based approach of Cole & Kuhlmann (2012) and the risk-based approach of IATA's "Check Point of the Future".

8. CONCLUSION

In summary, it is abundantly clear that the present rigid and predictable "one-size-fits-all" approach to airport security is not a desirable situation for screening today; neither will it be for the next generation of airport security (IATA, 2013). The industry needs to move from today's approach to airport security screening to a new approach that focuses on security outcome, process improvement and technology. One can forecast that the approach to airport security by 2030 will be different from the current approach.

The IATA concept of the "Checkpoint of the Future" and the Cole & Kuhlmann (2012) concept of scenario-based approach to airport security are not mutually exclusive of each other. They both advocate for a departure from the present approach of uniform airport security screening applied the same way to all passengers irrespective of their levels of risk. The new approach to airport security will not be "one-size-fits-all" but it will be based on passenger differentiation, supported by a scenario-based approach. Airport security approaches recently adopted by key global aviation stakeholders support IATA and Cole & Kuhlmann perspectives. Recently, the American Transportation Security Administration (TSA) acknowledged a move toward pre-screening in order to separate passengers and baggage that do not require extra layers of screening (Grimaldi, 2012). Also, ICAO and the Global Air

Cargo Advisory Group (GACAG) have agreed to support a risk-based approach to be adopted by airlines and cargo forwarders for security screening at airports (Grimaldi, 2012).

Given the success of the proactive approach in aviation safety through the implementation of safety management system (SMS), it can be predicted that a similar proactive approach may be considered before 2030 for airport security within the global aviation security community. There will be a push for the adoption of a Security Management System (SeMS) that will help regulators, governments and other aviation stakeholders measure the effectiveness of airport security policies and also create a security culture in organizations such as airports and airlines.

One can also forecast a future approach to airport security where various individual government standards and regulations related to airport security are harmonized into globally accepted standards that eliminates redundancies and duplications that are currently observed. Passengers and airlines will benefit greatly from the global airport security standards based on internationally agreed upon standards (IATA, 2013).

References

- Cole, M. and Kuhlmann, A. (2012) A Scenario-Based Approach to Airport Security, *Futures,* 44(4): 319–327.
- Elliot, J. (2009). 'Biometrics and Airport Security', *Biometric Technology Today*. October 2009, 7-8.
- Gold, S. (2012), 'Border Control Biometrics and Surveillance', *Biometric Technology Today*. July/August 2012, 9-11.
- Grimaldi, C. (2012), 'ICAO, Cargo Group to establish Risk-Based Security Rules', *Aviation Daily,* October 22, 2012.
- Holbrook, E. (2010), 'Airport Security: Privacy vs. Safety', *Risk Management*, 57, 2.
- Houdeau, D. (2009), 'Travel, borders and Immigration' *Biometric Technology Today*. October 2009, 8-11.
- International Air Transport Association (2013) *Checkpoint of the Future: Executive Summary.* Available from: http://www.iata.org/whatwedo/security/pages/checkpoint--future.aspx / (accessed on 25/01/2013).

- Kirschenbaum, A., Mariani, M., Gulijk, C.V., Rapaport, C. and Lubasz, S. (2012).'Trusting Technology: Security decision making at airports', *Journal of Air Transport Management*, 25, 52-60.
- Ott, J. (2010). 'Letting Loose', *Aviation Week & Space Technology* 172, 37.
- Peters, K. (2013). *Napolitano: Aviation Security tops DHS Priority List*. Available from: http://www.govexec.com/defense/2010/01/napolitano-aviation-securitytops-dhs priority-list/30732/ (accessed on 26/01/2013).
- Stolzer, J. A., Halford, C.D. and Goglia, J.J. (2008). *Safety Management Systems in Aviation*. Ashgate, Burlington, USA.
- Vasigh, B., Fleming, K. and Tacker, T. (2008). *Introduction to Air Transport Economics, from Theory to Applications*. Aldershot, Ashgate.
- Vogt, W.P., Gardner, D.C. and Haeffele, L.M. (2012). *When to Use What Research Design*. New York, The Guilford Press
- Wikipedia (2013), *Airport Security*. Available from: http://en.wikipedia.org/wiki/Airport - security/ (accessed 23/02/2013).