Journal of Air Transport Management 48 (2015) 34–41

Contents lists available at ScienceDirect

Journal of Air Transport Management

journal homepage: www.elsevier.com/locate/jairtraman

The social foundations of airport security

Alan (Avi) Kirschenbaum

Kirschenbaum Consulting Ltd, Israel

ARTICLE INFO

Article history:
Available online 27 July 2015

Keywords:
Airports
Security
Human factors
Security decisions
Trusting technology
Rule compliance
Airport organization
Social networks

ABSTRACT

Aviation security relies on the assumption that risks can be mitigated through rule compliance. To assure this, the operational design and logistical process has fashioned airports into mass production organizations where human behaviors – of both employees and passengers – are defined within a rational and logical framework. However, recent empirical evidence raises some critical issues as to the very basis of these assumptions. Employing the analysis of data obtained from 8 airports across Europe by ethnographic, field survey questionnaires, interviews and a cohort panel study, it is clear that bending and breaking the rules is fairly commonplace; most threats are assessed as false alarms; security decisions are predominantly group decisions; co-workers and friends influence rule compliance and passengers are active participants in security decisions. These behaviors certainly do not fit neatly into the classical model of airport design and operations. We will therefore argue – on the basis of the data generated from these methodologies - that the classical aviation security model should be extended to take into account the reality of human behavior of both passengers and employees in the security process. This approach emphasizes the social content within which security decisions are made, namely that airports, as complex social organizations, are composed of both formal administrative and informal social network structures. Organizational behaviors within these social contexts foster how security decisions are made and the degree they are rule compliant. We therefore expand the basic security model but give it added value by reflecting the reality of human behavior within an airports organizational context.

1. Introduction

When entering an airport, most passengers are unaware of the complex technical and human infrastructure that is in place to mitigate potential security threats. This organizational infrastructure does not, however, guarantee that in case of a crisis, all the key players will make appropriate or coordinated decisions to assure the security of the airport, its employees and passengers. Nor does it guarantee that the plans that were developed will be followed (Comfort et al., 2010; Barbash et al., 1986). This perspective reflects the reality of everyday airport operations when security employees and managers require the necessity for on-the-spot judgments to be made under extreme time pressure; especially when such decisions will have far reaching consequences on maintaining operational viability and 'bottom-line' sustainability.

Yet, airport architects in tandem with security professionals have traditionally designed airports that marginalize, and in effect, avoid this reality of security decision making by employees and behaviors of passengers. They have done so by designing structures based on mass processing engineering that heavily leans on technology and logistics (Horonjeff et al., 2009; De Neufville, 1995). From a security perspective, the level of airport security is seen in terms of taking advantage of technology to promote rule compliance to enhance safety and security that is promulgated by federal regulators (TSA, 2011; GAO, 2005). Greater rule compliance in this framework means greater airport security. More sophisticated security technology brings with it additional security assurances. Together, mass processing through systems engineering and the assumptions that passengers and employees are “passive cogs” to be manipulated formed a basis to remove as far as possible the human element in security decision making. From an engineering perspective, reducing human intervention in the security decision making processes is the optimal objective (Harris, 2002). To this end, technology has become a substantial mechanism to maintain rule compliance by removing decisions from airport employees by leaving the decisions in the hands of sophisticated security software. Such software can not only detect objects that present potential threats but to some extent also behavioral abnormalities that can be interpreted as threats (Meservy et al., 2005). This

E-mail address: avik@tx.technion.ac.il.

http://dx.doi.org/10.1016/j.jairtraman.2015.06.010
0969-6997/

perspective fits in well with the basic approach toward security outlined by all the major security agencies and regulatory bodies (TSA, 2011; EU, 2006; FAA, 2013). When rules are kept security is maintained; when not complied with the airport is put at risk. And, to a large extent, this security goal has been met at most security check points throughout the airport. Yet, despite the attempts to minimize human based decision making in matters of security at airports, evidence is accumulating that this effort has not been fully successful; thereby increasing the risks of a breech in airport security.

2. Classic human factors

With the continuous development of more refined security hardware and sophisticated software has come a similar need to seek ways to simplify operating procedures for a broad range of security employees (Langan et al., 2009). One approach toward the goal of minimizing human intervention in security decisions has been sought in the area of ergonomics and human factors engineering. The aim of both is to design security technology so as to reduce the need for human intervention in both the operation of the technology and reducing complexity in having to make decisions. What has evolved is that classical human factors add a psychological dimension into the engineering design that attempts to find a better fit between machine and man so as to reduce cognitive effort and optimize physical ease in operation (Svenson and Maule, 1993). It for this reason that many security devises, be they based on output signals or interpreting x-ray images; are designed to simplify, and in many cases eliminate, the need to interpret complex output signals. To this end, a green vs red light, dark spots on a stick figure for total body scans as well as audio and visual cues are all provided through very sophisticated software but require minimum cognitive ability to interpret the output. This same principle applies to software for behavioral detection. A large amount of effort has been put into applied research in this area, particularly in the screening of passengers and baggage (National Research Council, 1996)) with most of the effort directed at visual interpretation of the output signals from various screening devises (Patankar and Holscher, 2000). The overriding goal, in this case, is to minimize the time required to determine threat levels of passengers or other non-human items to be transported. This system is also utilized as part of controlled logistic systems to direct and insure the location of passenger flow as well as insuring that passengers and their baggage embark on flights together. By accomplishing this, airport managers can claim that “throughput” increases, security costs decrease, and as the number of passengers flowing through the airport increases so do revenues! Yet, despite all the efforts to optimize man-machine interaction in the use of security technology, it is recognized that this approach is bounded as it ignores the non-machine social context within which security decisions are made (Kirschenbaum et al., 2013) as well as the employee's own degree of trust that the security devise is accurate (Worley et al., 2000). False alarms are not only software glitches due to probabilistic errors in programming but also in the uncertainty that affects the human operator perceptions. These will be discussed in more detail below but it is fair to state that bending and even breaking the rules and/or protocols is done frequently enough to warrant the distinct possibility the decision making process cannot be reduced to simple man-machine single-individual interactions alone.

In addition, making security based judgments even under a strict rule compliance framework leave ample room for bending or even disregarding the set administrative rules. But would this also hold in terms of security technology where decisions have been automated? Here, it is not the trusting of the actual physical technological apparatus itself but in trusting the output signals of the technology that may affect actual compliance behaviors. This distinction is important because technology acts as detectors of security threats; they can be seen as instruments that provide employees with information that should make sense (Weick Sutcliffe, 2001). But employees may find themselves in situations when the output of the security technology may not match the situation. The classic example of liquid medication exceeding the allowed size but needed by an elderly disabled person during a flight. Or the agitated and nervous passenger who turns out to be late for a flight and not a terrorist. It is here that trusting the technology or utilizing its output as one of alternative means in making a security decisions becomes paramount.

3. Airports as social organizations

3.1. Formalistic structures

In order to understand the link between security technology and security decisions, it is vital to recognize that airports are socially based economic organizations composed of complex and interdependent groups of decision makers (Remawi et al., 2011). By law, regulators determine security formats in airports, resulting in a command-control like structure that guide how rules and protocols are administrated (IATA, 2014). This imposed design has led to an architectural approach hinging on engineering mass processes. The result has been recognized by scholars of organizational behavior as representing an organization built along formalistic structural foundations. As an initial and pervasive explanation for the basis of organizing behavior, it reflects what has been termed the *rational system* approach. This approach assumes a high degree of rationality in human behavior that is directed toward purposeful goal seeking. Given this approach, the organizing ability of modern man to deal with crises (or security threats in the case of airports) should generate a foolproof management organization, capable of dealing with every imaginable type of threat. The emergent structure that would evolve is likely to have classic characteristics of what we call today a bureaucracy: a hierarchical structure, authority associated with the office, defined power relationships and a top down chain of command. This approach toward organizing has several variants. One focuses on the scientific rational utilization of the individual who is seen as a cog in a well-oiled machine. Here, Frederick Taylor's classical “scientific management” approach (Scott, 2004; Daft, 2008) represents this viewpoint. This rationalistic approach is buttressed by emphasis on the rational use of administrative directives where (Henry Fayol's 14) principles of administrative management maintain the structural integrity and operational continuity of the organization. In addition, to a highly formalistic framework comes rational options for decision-makers that forms the basis for organizational success. The underlying theme of all these organization forms is that rational behavior determines the best structure, means and processes through which the organization attains the groups' goals. Within this ideal structure, rational decisions take place that expedite performance. In the case of both the design and operation of airports, this “rational” approach has taken credence over other alternative means to deal with maintaining operational viability. Yet, as I have pointed out above, empirical evidence is accumulating that demonstrates that this model of organizing airports, especially in terms of security, is far from ideal.

The Achilles heel of the rational approach in organizing behavior is that it disregarded many non-rational characteristics of people. The “ideal” rational man faced the reality of human social life. Taking this cue, organizational researchers forcefully argued that organizations mirrored the social dynamics inherent in societies.