Journal of Air Transport Management 25 (2012) 57–60

Contents lists available at SciVerse ScienceDirect

Journal of Air Transport Management

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

Note

Trusting technology: Security decision making at airports

Alan (Avi) Kirschenbaum [a,*], Michele Mariani [b], Coen Van Gulijk [c], Carmit Rapaport [a], Sharon Lubasz [a]

[a] Technion – Israel Institute of Technology, 32000 Technion, Haifa, Israel
[b] University of Modena e Reggio Emilia, Italy
[c] Delft University of Technology, Netherlands

Keywords:
Airport security
Airport employees
Trust
Security rules

ABSTRACT

Using data from a field survey of airport employees across European airports, we identify how trust in security technology affects the implementation of security rules and regulations. An analysis of respondents from eight airports in Europe demonstrated that compliance with security rules and protocols was related to two main categories of trust in technology: one oriented to the technology itself and the other to technology as a means of catching offenders. A further multivariate analysis showed that security decisions by each 'trusting' group tended to reflect its degree of commitment to the organizations' administrative guidelines and the organizations' security attitude.

1. Introduction

The utilization of security technology in airports to detect security threats to travelers and airport facilities is embedded in an organizational framework that links technological output to sets of rules and regulations that govern security employee's behavior. This organizational framework is designed to provide a functional and complete working environment for a security risk management resilience system.[1] (Talbot and Jakeman, 2009). Under ideal conditions such technology and compliance with rules and protocols associated with its output should provide adequate protection against potential threats. Yet, recent evidence in airports has shown that this is not always the case (Kirschenbaum et al., in press). There are a consistent and fairly large proportion of airport security employees who utilize security technology but bend the rules and even break them if the situation calls for it. One potential explanation for non-compliance may be based on how employees interpret the technology's output, particularly the degree that employees "trust" the technology; be it trusting the technology completely or perceive it to be the best way to detect threats (Brooks, 2010). We theorize that when such technology is not trusted, there is a higher likelihood that non-compliant security decisions are made. To test this argument, we will explore how and what way "trust" in security technology affects airport security decisions. The implications are far reaching for airport security as well as diverse types of transportation security operations.

2. Trusting technology and rule compliance

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). This means that making security based judgments even under a 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 and 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. It is here that trusting the technology or utilizing its output as one of alternative means in making a security decisions becomes paramount.

* Corresponding author. Technion – Israel Institute of Technology, 32000 Technion, Haifa, Israel. Tel.: +972 4 9931310; fax: +972 4 8295688.
E-mail address: avik@tx.technion.ac.il (A.(Avi) Kirschenbaum).

[1] The basic underlying assumption made by policy makers and managers alike for maintaining high levels of security rests on an administrative framework governed by both internal organizational rules and protocols as well as externally imposed directives generated by legal authorities.

0969-6997/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.jairtraman.2012.08.005

3. Methods

Given the above alternative perspectives of what trusting technology entails, we have posited a simplistic theoretical working model (See Fig. 1) which will guide us in our analysis. The model basically argues that trusting technology is a two-pronged construct that may reflect employees complete trust in the security technology devise itself and/or the perception of technology as a means of obtaining output upon which a security decision can be made. The dominance of an employee's trust toward one view of technology or the other will, in our model, have an impact on the likelihood that compliance with the security rules and protocols will be adhered too. Thus, in order to explore how trusting technology affected actual behavior of security related decisions made by airport employees, we generated a series of studies at various international airports in Europe, varying in size and traffic volume, and across different national states and cultures. The first step was an exploratory ethnographic study which laid the foundation for a pilot study and then comprehensive structured questionnaire survey. We used the ethnographic study to provide the raw social data based on actual behavior for understanding the social processes involved in security related activities in airports. Over 250 separate observations were recorded in a number of airports that included a diverse number of air and land sites. Many of the observations incorporated multiple scenarios so that an initial calculation was that over 700 separate behavioral items were extracted and described in detail from the ethnographic observations.[2]

Based on the analysis of the ethnographic study, a full scale field survey based on an extensive and detailed questionnaire was given to a purposely chosen sample of 514 employees distributed throughout the airports' occupational structure at eight (8) airports purposely selected on the basis of their size, distribution and cultural diversity. The structured questionnaire covered a broad range of potential constructs which were discovered in the initial ethnographic observations involved in security decisions. The basis for the measures was linked to our assumption that airports are social organizations that would reflect multiple organizational behaviors generated within its formal and informal structures. A pilot questionnaire survey first tested the reliability and validity of the measures. In certain cases, the questionnaire was translated into the dominant language where the airport was located. The questionnaires were anonymous to meet the ethnical code of the Helsinki Protocols and given out and collected in the same day when possible.[3] In our case, a part of the questionnaire was used; those measures that were relevant for investigating trust in technology. Two key measures of "trusting technology" were employed: Respondents were asked if "I put my complete trust in security technologies?" based on a dichotomous ''yes–no' response. In addition they were asked if "Technology is the best way to catch security offenders?" based on a 4 value Likert type scale from 'completely agree' to 'completely disagree'. The choice of two measures of 'trusting technology' reflected two key perspectives found in the trusting literature: one focusing almost exclusively on the technology itself (complete trust) and the other on the output of the technology (best way to catch offenders). In this way it was possible to not only distinguish how each affected compliance with security decisions related to technology but search for the sources of such decisions.

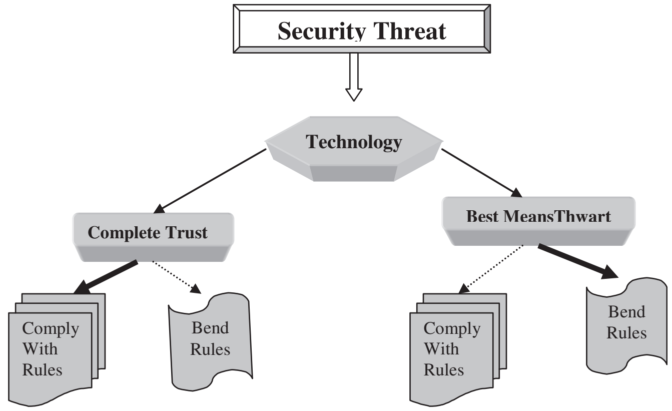

Fig. 1. Theoretical working model of security decision making tree linking trusting technology and compliance to security rules.

We also employed three measures of compliance. The first level was based on measuring the degree to which an employee was "bending the rules" asking the question: "I would exceed or bend the rules if the situation called for it". The second level of compliance went beyond just bending the rules but actually "breaking protocol is sometimes necessary". The third level of compliance reflected an even more deviant behavioral pattern as was measured in terms of the question "I would even act against orders" .In all cases a four value Likert type scale from completely agree to completely disagree was measured. Overall, the characteristics of the sample showed that most were male (65%), having an average age of 36.5 years with most under 30 years of age and close to half (42%) married with about a third single (38%).

4. Results

4.1. Compliance with rules

In general, the questionnaire survey results point out that a considerable proportion of the sample had doubts about the ability of security technology to be effective. We found, for example, that just over half (52.4%) of the respondents stated that they put their *complete* trust in technology. In terms of agreeing with the statement that technology is the best way to catch security offenders, the split was toward agreement (51.7% mostly agreed and 14.2% completely agreed) but with still a third disagreeing with the statement (24.4% disagreed and 9.7% completely disagreed). We took these results and explored possible relationships between the compliance behaviors. As usual when using ordinal and interval type data sets, we employed Pearson correlations and Chi Square non-parametric types of analysis. These obviously do not provide the predictive direction of the relationship but do establish the importance of the relationship. What we discovered was the association between them proved to be highly and positively significant confirming that employees who put complete trust in technology also tend to agree to trust its ability to catch offenders. These findings are cross-referenced with parameters that relate to rule bending: "exceeding or bending the rules" and "would act against orders" which is also significantly correlated as well as correlates with "break rules if necessary". This can initially be interpreted to mean that there appears to be a split among the respondents in terms of their willingness to keep or bend the rules.

[2] For more details of the ethnographic method and the results, see Kirschenbaum et al. (2012a). The ethnographic study was based on three airports with scripts recorded and categorized by a team of judges. This data set was then analyzed by a software program designed for qualitative data analysis.

[3] It should be noted that the results of an analysis of the ethnographic study closely matched the results of the later performed questionnaire survey providing interactive empirical support for the overall findings.