University of Huddersfield Repository

Kirschenbaum, Avi, Mariani, Michele, Van Gulijk, Coen, Rapaport, Carmit and Lubasz, Sharon

Airports at Risk: The Impact of Information Sources on Security Decisions

Original Citation

This version is available at http://eprints.hud.ac.uk/23350/

http://eprints.hud.ac.uk/

Journal of Transportation Security

Airports at Risk: The Impact of Information Sources on Security Decisions
--Manuscript Draft--

Airports at Risk: The Impact of Information Sources on Security Decisions

Alan (Avi) Kirschenbaum
Technion- Israel Institute of Technology
Faculty of Industrial Engineering and Management
Haifa 32000, Israel.
avik@tx.technion.ac.il

Michele Mariani
University of Modena e Reggio Emilia,
Viale Allegri, 9, 42100 Reggio Emilia, Italy.
michele.mariani@unimore.it

Coen Van Gulijk
Faculty of Technology, Policy and Management
Delft University of Technology, Netherlands
C.vanGulijk@tudelft.nl

Carmit Rapaport
Technion- Israel Institute of Technology
Faculty of Industrial Engineering and Management
Haifa 32000, Israel.
carmitr@tx.technion.ac.il

Sharon Lubasz
Technion- Israel Institute of Technology
Faculty of Industrial Engineering and Management
Haifa 32000, Israel.
slubasz@gmail.com

Corresponding author: Alan (Avi) Kirschenbaum avik@tx.technion.ac.il, Mobile:

972-54 766 9399, Fax: 972 49931310

1

Abstract

Security decisions in high risk organizations such as airports involve obtaining ongoing and frequent information about potential threats. Utilizing questionnaire survey data from a sample of airport employees in European Airports across the continent, we analyzed how both formal and informal sources of security information affect employee's decisions to comply with the security rules and directives. This led us to trace information network flows to assess its impact on the degree employees making security decisions comply or deviate with the prescribed security rules. The results of the multivariate analysis showed that security information obtained through formal and informal networks differentially determine if employee will comply or not with the rules. Information sources emanating from the informal network tends to encourage employees to be more flexible in their security decisions while formal sources lead to be more rigid with complying with rules and protocols. These results suggest that alongside the formal administrative structure of airports, there exists a diverse and pervasiveness set of informal communications networks that are a potent factor in determining airport security levels.

Key Words: Airports, Security Decisions, Information Sources, Social Networks

2

Airports at Risk:

The Impact of Information Sources on Security Decisions

Introduction

Airports, as complex social organizations, are mainly characterized as having a formal social structures bolstered by a legal set of administrative rules that affect its operational maintenance and continuity. Little emphasis is put on the rich fabric of informal networks that also play a critical role in airport management. We argue that these two forms of social structures provide in tandem the conduits for the selective flow of information through both formal administrative channels as well as informal social networks (Handel, 2002) that will affect the level of airport security. For airports, not only does the flow of information affect daily operations but it can also have a direct impact on security decisions (Huang et al, 2011). On the one hand, the formalistic administrative structure underpinning security decisions in airports is dominated by sets of clearly enunciated rules, regulations and protocols that are designed to determine security decisions. On the other, are the informal social networks that are generated through employee interactions within and between work units and departments (Crampton et al, 1998). In cases when a security decision needs to be made, it would seem that formal sources of information – given its legal and administrative prerogative - should marginalize information generated through informal social networks. Yet, recent ethnographic evidence has shown that informal social interactions in airports are alive and have an impact on group based security decisions making (Kirschenbaum et al, 2012), along with a great deal of bending and even breaking the rules (Kirschenbaum et al, 2012a).

To what extent do such informal sources of information impact on security decisions is not clear but these finding raise serious questions as to the veracity of the official formal sources as the sole determining factor is such decisions. In order to clarify this issue, we will explore and evaluate the degree that formal and informal sources of information within an airport organizational framework impact on security related decision making among its employees. Simply put, does the security information obtained through your friends have a greater impact on decisions than those coming through the chain of command?

The relative importance of informal social networks as sources of valuable information affecting behavior is not new (Kraut et al, 1990). But the degree of is influence during periods of crisis or threatening situations is less well documented. Recent evidence in the area of organizational behavior has shown the impact that both formal and informal social networks have on a range of decisions made during crises (Krackhardt and Stern, 1988). In the area of disaster management, scholars have pointed out how the flow and choice of both formal and informal sources of information can make the critical difference for survival. Such decisions include situation when evacuation, taking shelter and making preparations for various conflicts is required. What these and other studies have demonstrated is that

3

critical decision making in cases of threats – be they human made or natural – depends to a great extent on the sources of information available and the choice to utilize them. These same choices, we contend, are also available within the organizational framework of airports. The aim here will therefore be to first discover the degree that informal information flow networks exist within the formal airport structure and then examine the degree to which such informal sources of security information act in influencing security decisions.

Structure of Airports

Unlike the simplistic descriptions of airports as consisting of "airside" and "landside" sites, we argue that airports, as complex socially based economic organizations, have characteristics similar to all complex social organizations. One critical characteristic that will help in understanding how information sources affect security decisions is the existence of formal and informal internal communications networks. The formal structure typically seen in organizational charts reflect the legitimate administrative rules that determine the flow of command and power. The example of a subordinate either receiving orders (e.g., information) from her/his boss or passing on information to the boss and not through others as the administrative structure dictates reflects this type of formal structure. The informal structure, however, is more a product of social interactions that are generated within the various levels of the airports organizational setting and can be distinguished by the fact that it is through these social interactions – and not administrative directives – that its distinct network develops. The emergence of informal leaders, across departmental interest groups and informal channels of information flow develop as an alternative path of communications within the organization. In each case, the flow of information that maintains operational continuity follows different paths; one path is dictated by the formal administrative rules and protocols and the other through a loose set of recognized social networks based primarily on friendships and acquaintances. In many cases both types of communications networks are employed conterminously and even simultaneously (Varda et al, 2009). Therefore, making judgment decisions, especially under extreme pressure to keep flight timetables on schedule, can lead to bending or even disregarding the given set administrative rules (Angenendt, 2003).. These issues are complicated by the variety of potential security threats inherent in airports as major transportation hubs, and the multiple organizational levels in the airport administration that must make decisions when a crisis occurs.

This point should be emphasized as the complexity of managing the decision making chains that are an integral part of the airport organizational structure is complicated as multiple stakeholders are involved in airport crises management. This opens possibilities for conflicting interests and communications disruptions (Butts et al, 2007; Corbacioglu & Kapucu, 2005). For example, airport authorities want to maintain security but to do so may conflict with airline carriers wanting to keep to their schedules, passengers demanding little or no delays, control tower personnel seeking minimum disruption over air space and service providers wanting easy access for employees without going through security checks.

4

Information Flow

Recent evidence on security decision making in airports has shown it to be primarily based on interactive group decision making (Kirschenbaum et al, 2012). These findings, along with the variability among employees in complying with the rules and protocols, strongly suggest that information sources for security decisions not only occur within the province of formal administrative network structure but also outside it. This possibility is supported by studies of manufacturing, service and public organizations which clearly describe the intermixture of both formal and informal information networks found at all levels of the organization (Kirschenbaum & Rapaport, 2008). The importance of internal company sources of information, for example, was found to be important in policy and operational decisions (Keegan, 1974). In terms of internal organizational networks, a search for relevant material may be related to the risk involved for the searcher (Blay, et al, 2012). Another study focused on how security behavior could be affected by an internal security threat in contrast to external security threats (Leach, 2003).

In the case of emergencies and disasters, informal networks were found to be critical in maintaining operational continuity (Rapaport & Kirschenbaum, 2008). Given the likelihood that the source of information affecting an airport security decision may emanate from either or both formal and informal sources, there arises the possibility that the source may have an impact on what kind of decision is likely to be made.

The possibility that sources of information affect decisions is not new. Studies of small group dynamics as well as analysis of social networks in large organizations have clearly demonstrated the impact of information sources on decision making (Kraut et al, 1990). In general, the complexity of the organizations size and structure has an impact on the density of the informal social networks which act as conduits for information distribution. But more importantly, these studies have made it clear that informal sources of information generated within the organization have also different levels of perceived risk (Blay et al, 2012; Haung et al, 2011) as well as a differential impact on incentives, penalties, peer pressures and perceived effectiveness that impact upon compliance levels (Herath & Rao, 2009).

In a sense, the formal networks are bolstered by administrative legitimacy but the informal social networks by trust. Thus, information passed along by friends or coworkers with whom the employee has a long association of mutual interaction appears to be seen as more reliable than simply "orders" or "protocols" from an unknown, anonymous administrative source or even their direct boss (Willemyns et al, 2010).

Levels of Rule Compliance

5

If we put the emphasis on compliance to rules or protocols themselves and not specifically to security decisions, we find that low compliance is very common (Haynes & Dantesa, 1987) with individuals simply not complying with directives or orders (Morris & Schulz, 1992). One possible but promising explanation why certain people follow the rules and others do not has been put forward by utilizing theories of Organizational Citizenship Behavior (Shropshire, 2009). For example, complying with security protocols may be motivated by something other than financial compensation. Others have argued that security technology itself brings about a lowering of compliance by the over reliance on machine output (Gonzalez & Sawicka (2003). At the organization level, the disaster literature points to a large gap between emergency and disaster plans and actual implementation (Kirschenbaum, 2004). Apparently, due to the dynamic changing situation during crises, pre-determined emergency plans and directives are usually discarded, implying that the protocols are in the main ignored. If this is the case, it is reasonable to expect similar patterns of non-compliance to the emergency rules and protocols in high risk organizations such as airports.

As the research literature on compliance has predominantly focused on health care, it is not surprising that this concept has been viewed in terms of a bipolar measure: total compliance with instructions or non-compliance. In the jargon of the physician, "Did you take the medication or not?" Yet, this concept can certainly be viewed in more subtle terms such as "partially complying". This would broaden the range of potential compliance behaviors and provide an in-depth understanding of its variability. A closer examination of the construct 'compliance', especially as it relates to airport security, led us to reevaluate its general meaning and look for more subtle measures. A recent ethnographic study of airports clearly showed that compliance came in many shades; completely following the rules as to actually disregarding and even acting against them (Kirschenbaum et al, 2012). This led us to take a three pronged approach by deconstructing this concept in terms of various levels of actual behavioral compliance to the (semi) legal administrative directives (figure 1). 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". Overall, we were able to decipher three significant levels of compliance to security directives allowing us to assess the degree to which each of the formal and informal sources had an impact on each compliance level. Our initial hypotheses argued that as security information was sought more from informal rather than formal sources, the tendency to deviate from the rules becomes more pronounced.

6

Security Situation Requiring Decision

| Compliance | Exceed or Bend Rules | Break Protocol | Act Against Orders |

Minimum ⟸ Levels of Non-Compliance ⟹ Maximum
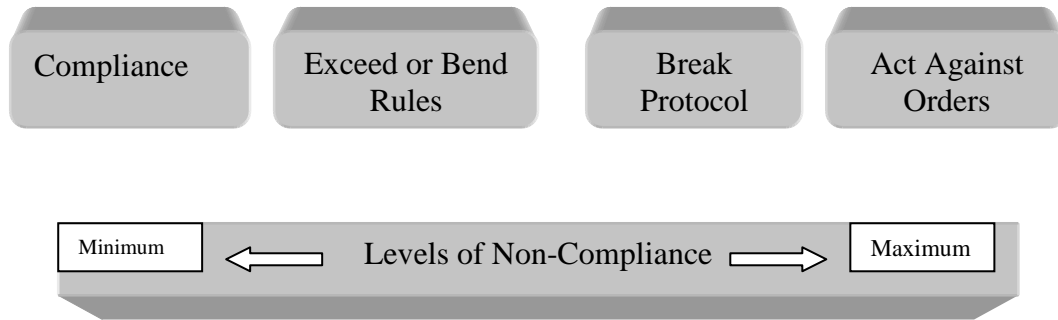
Figure 1: Security decision levels

Methods

To test our argument that there will be differences in decision compliance with security directives as a result of the source of information utilized in that decision - either through formal or informal networks - we have posited a theoretical working model (See Figure 2) which will guide us in our analysis.

Figure 2: Basic Working Model of Impact of Information Sources on Security Decisions

7

Structure of Organization ⟷ **Organizational Environment**

Communication
Networks

Formal Sources → **Information** ← Informal Sources

Security Decisions

Compliance   Non-Comply
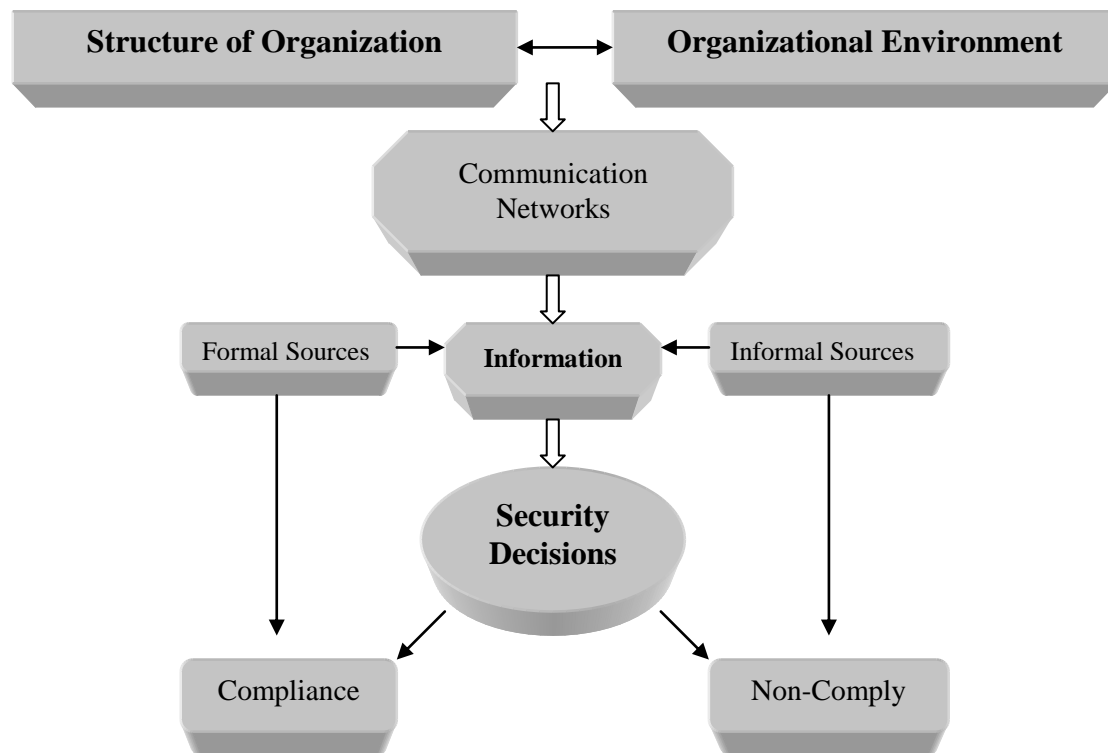
The model basically posits that within an airports' organizational environment there are available multiple sources of information concerning threats and alternative actions. These sources of security related information flow through a communications network that is either generated within the formal administrative structure of the airport organization (top-down or bottom-up) or through its informal conduit of social networks, for example, social gatherings during breaks,. Depending on the choice of source, we argue that an employee will make a security decision that will either comply or not with the rules and protocols generated by security agencies. Simply, the dominance of an employees' use of one source or the other, 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 the veracity of this argument, we generated a series of studies at a number of international airports in Europe, varying in size and traffic volume, and across different national states and cultures.

Data Sources

The data collected was based on three separate but interconnected sources. The first was an analysis of ethnographic observations followed by a full scale field survey grounded on an extensive and detailed questionnaire given to a purposely chosen sample of 514 employees at the airports (Kirschenbaum et al, 2012). This was followed by detailed personal interviews of over 360 security employees aimed at deciphering among other issues, the information flow network among employees. The overall characteristics of the sample showed that most were male (65%), having an average age of 36.5 years

8

(SD=21.1) with most under 30 years of age and close to half (42%) married with about a third single (38%).

The ethnographic study provided a general overall picture of the reality of employee behavior in the airports providing the basis for developing the structured questionnaire that covered a broad range of potential constructs involved in security decisions. The interviews were based on (70) open ended questions that provided basic information allowing us to determine both the formal and informal communication networks in the airports. Employing a networking analysis tool based on asking "who do you typically go to for advise" and "who typically approaches you for advise" when a decision needs to be made demonstrated that such informal communications networks exist within and between airport units and departments and provide an alternative means of seeking and obtaining relevant information.

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. In our case, a part of the questionnaire was used; those measures that were relevant for investigating sources of information.

Key measures of "sources of security information" were employed. Respondents were asked if "I receive information about security threats" from "my direct boss", "through friends", "through rumors" "from briefings" "from written orders". In addition, we also tapped into questions that probed if they obtain security information "from friends outside the department" and "during meals and coffee/cigarette breaks". The first set of measures is based on a dichotomous 'yes-no' response. The second set of two measures is based on a 4 value Likert type scale from 'completely agree' to 'completely disagree'. The choice of these measures reflected two key perspectives found in the literature: one focusing on information that was obtained through formal administrative networks: "direct boss", "from briefings" and "from written orders". A second set of measures is aimed at discovering the extent of informal social network information sources such as obtaining information "from friends", "through rumors", "friends outside the department", and "during coffee breaks". This allowed us to distinguish how formal and informal sources of security information affected compliance with security decisions. In the case of the compliance measures, each was measured as a Likert type four (4) value scale ranging from "completely agree" to "completely disagree".

This distinction between communication network flows originating within the formal structure of the airport and that generated through social network interactions outside this framework is also obviously dependent on other sets of contingencies which will be examined employing a multivariate regression model. These variables have been cited as possible moderators in the link between security sources and actual decision making. They include in particular the impact of group or individual security decisions

9

external social network inputs, past experience encountering threats and if security information makes a difference in the decision.

Results

In terms of the impact that security information had on their behavior, it appears (see Table 1) that such information is a critical component in making security decisions. Over 80 percent of the sample responded in the affirmative – agreeing or completely agreeing - that such information affects what they do on their job. Even when differentiating between those employees who state their job descriptions as security related to those who do not deal directly with security, the importance of information remains high; 90% against 65% (χ =0.000)

Table 1: The security information I get affects what I do on my job

	Security Employee	Non-Security Employee	Total
Completely disagree	3.4%	21.1%	8.3%
Mostly Disagree	7.6	14.8	10.5
Mostly Agree	43.2	43.7	42.9
Completely Agree	45.8	20.4	38.3
Total Percent	100.0%	100.0%	100.0%
N	354	142	496

This confirmation of the value of security information in making a security decision led us to a next step that involved deciphering the source of the information. To do so we asked the respondents from whom they received such information. The results (Table 2) reveal that information sources vary from official formal conduits to informal sources such as friends and rumors. When asked where the employee obtains most of his security updates, we note that the prime source are two formal sources, namely the direct boss (70.8%) followed by written orders (63%). Simultaneously, nearly half also state that they also obtain updates from friends (53%) and even rumors (33%). In a sense, what we are seeing is that both the formal and informal communications networks provide a source for security updates.

10

Table 2: Measures of Formal and Informal Sources of Information "I get most of my security updates from…" (N= 514)

Formal Networks	Yes	No	Total
My boss	70.8%	29.2%	100%
Formal briefings	52.6	47.4	100%
Written orders	63.0	37.0	100%
Informal Networks			
Friends	52.9	47.1	100%
Rumors	33.9	66.1	100%

Information and Non Compliance

Employing separate linear regression models that encompasses each of the three levels of " non compliance" as the dependent variable against the entire alternative formal and informal security information sources clearly and strongly suggested that the type and source of information an employee attains has a direct and significant impact on the degree to which she/he complies with the security rules and protocols. (Table 3). More closely evaluating the results shows that the significant determinants of both compliance and variations of non-compliance are concentrated in three key independent variables: (1) the clear expression that security information does have an impact on a decision; (2) information accessed through formal channels through the employees' boss and (3) from informal channels reflected in friends in other departments. From the size of the coefficients and significance levels, it can also be seen that the (1) impact of information is only marginally significant ($p<0.10$) while accessing information through (2) formal channels and (3) informal channels are highly significant (p.0.001) in terms of compliance levels. It should be noted that these levels of significance range across all the compliance levels.

The data in Table 3 also reveals a pattern of behavior that points toward the impact of both formal and informal communications networks on compliance. For one, the signs

11

Table 3: Summary of Comparative Regression Models of Compliance

	Bend Rules	Break Protocol	Against Orders
	B	B	B
(Constant)	2.482	2.565	2.047
The security information I get affects what I do on my job	-.115*	-.124**	-.091
I get most security information through rumors	.001	-.024	.013
I get most security information Mainly through my boss	-.089	-.155**	-.086
I get most security information from friends OUTSIDE the department	.218**	.210**	.222**
I get most security information During meals and coffee/cigarettes breaks	-.060	-.013	.007

1. I exceed or bend the rules when the situation calls for it
2: Breaking protocol is sometimes necessary to get the job done
3　Would even act against orders
*P<0.05
**P<0.01

of the significant regression coefficients are clearly indicative that information gleaned from informal sources lead toward minimizing rule compliance while those obtained from formal sources maximize such compliance. In addition, these patterns of compliance behaviors are significantly affected by the degree that an employee sees such information as important in making her/his security decisions.

Conclusions

Within the organizational framework of an airport, security decisions are made almost continuously. For the most part, these decisions involve routine decisions at security check points. Whenever a non-routine situation occurs, however, accompanied by a real or perceived threat, the decision making process can become complex and dynamic. It is at these times that situations arise when the routine rules and regulations may not neatly fit the circumstances. In these cases where a threat　emerges, decisions are theoretically governed by rules and regulations supported by the airports administrative structure. What has been established by recent research, however, is that compliance to the rules and protocols varies and ranges from complete compliance to total disregard of the rules. A possible explanation that was explored here focused on the source of security information that the employee utilized in making a security decision. By tracing the source of information, derived through formal or informal communications networks, we were able to discern how each type of information affected security rule compliance. The underlying working assumption was that both access to security

12

information and the degree of trust of the provider would affect how such information would be utilized in a security-threat situation.

The results of the analysis clearly showed that information is considered a vital component in how airport employees make security decisions. This was found to factor into decisions made that involved all levels of compliance, ranging from bending the rules, breaking protocol or even acting against orders. With this in mind, we also discovered the importance of where such information originated; be the formal or informal communications networks. Security information utilized from formal sources predicted high rates of compliance while information received from friends (through informal networks) toward more flexible and adaptive behaviors. As in any other complex organization, organizational process have a highly dynamic nature, and spontaneous informal social networks are continuously generated through employee interactions. In such a context, when a decision has to be taken, informal information networks play a critical role, especially with respect to the ability to cope with the unexpected

Implications

Our findings have far reaching implications on airport security. For one, an airport can no longer be solely viewed as a strictly formal organization governing the security behavior of its employees by imposing administrative directives. Rules and protocols are being bent, broken and disregarded. For another, security decision making appears not to be a rote training-like exercise but is influenced by the organizational origin of the information the employee obtains. Apparently there is a vibrant set of informal social networks in airports that provides alternative paths for accessing information and, more importantly directly influence the degree that the security protocols will be followed. Our results show a clear pattern where information sources emanating from the informal network tend to encourage employees to be more flexible in their security decisions while formal sources more rigid with compliance tending to follow rules and protocols. This in itself should make those who advocate a purely engineering-technology perspective of airports design and security to take a step backwards to reevaluate the degree that 'human factors' play in the reality of airport operations.

References

Angenendt,A. (2003). Safety and security from the air traffic control services' point of view. Human Factors and Aerospace Safety. 3(3), 207-209.

13

Blay, A.D., Kadous, K. and Sawers, K. (2012) The impact of risk and affect on information search efficiency Organizational Behavior and Human Decision Processes, 117(1):80-87.

Butts, C., Petrescu-Prahova, M., Cross, B. (2007). Responder Communication Networks in the World Trade Center Disaster: Implications for Modeling of Communication Within Emergency Settings. The Journal of Mathematical Sociology. 31, 121-147.

Corbacioglu, S., Kapucu, N. (2005). Intergovernmental Relations in Response to the 1999 Marmara Earthquake in Turkey. International Journal of Mass Emergencies and Disasters. 23, 73-102.

Crampton, S. M., Hodge, J. W., Mishra, J. M. 1998. The Informal Communication Network: Factors Influencing Grapevine Activity. Public Personnel Management, 27(4):569

Handel, M. J. (2002) The Sociology of Organizations Classic, Contemporary, and Critical Readings SAGE Publications, Inc

Herath, T., and Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2):154-165.

Gonzalez, J. J., and Sawicka, A. (2003) The Role of Learning and Risk Perception in Compliance. Proceedings 21st International Conference Systems Dynami Society, NYCity, July 2003.

Haynes, R.B. and Dantesa, R. (1987). Patient compliance and the conduct and interpretation of therapeutic trials. Controlled Clinical Trials. 8:12-19.

Huang, D., Patrick Rau, P., Salvendy, G., Gao, F., Zhou, J. 2011. Factors affecting perception of information security and their impacts on IT adoption and security practices. International Journal of Human-Computer Studies, 69(12): 870-883.

Kirschenbaum, A. (2004). Chaos Organization and Disaster Management. Marcel-Dekker, New York.

KirschenbaumA., Mariani, M.; Van Gulijk, C; Lubasz, S., Rapoport, C. and Andriessen, H. 2012. Airport security: An ethnographic study. Journal of Air TransportManagement18:68-73.

KirschenbaumA., Rapaport, C., Lubasz, S., Rapoport, C. Mariani, M.; Van Gulijk. (2012) Security Profiling of airport employees: complying with the rules. Journal of Airport Management 4(3):250-271.

Kraut, R. E., Fish, R. S., Root, R. W., Chalfonte, B. L. (1990). Informal Communication in Organizations: Form, Function, and Technology in I S. Oskamp & S. Spacapan (Eds.). Human Reactions to Technology: The Claremont Symposium on Applies Social Psychology. Beverly Hills, CA: Sage Publications.

Krackhardt, D. and Stern, R. N. (1988) Informal Networks and Organizational Crises: An Experimental Simulation Social Psychology Quarterly, 51 (2):123-140

Morris, LS, Schulz RM. 1992. Patient compliance--an overview. Journal of Clinical Pharmaceutical Therapy.17(5):283-95.

Rapaport C. and Kirschenbaum, A.. (2008). "Business Continuity as An Adaptive Social Process". International Journal of Emergency Management, 5(3/4):338-347.

Leach, J. (2003) Improving computer security behavior Computers and Security, 22(8):685-692.

Shropshire, J. D. (2009) Predicting compliance with prescribed organizational information security protocols. Dissertation Abstracts International Section A: Humanities and Social Sciences, 69(11-A)

Keegan, W. J. (1974). Multinational Scanning: A Study of the Information Sources Utilized by Headquarters Executives in Multinational Companies Administrative Science Quarterly , 19(3):411-421.

14

Willemyns, M , Gallois, C. and Callan, V. (2003). Trust me, I'm your boss: Trust and power in supervisor–supervisee communication. The International Journal of Human Resource Management. 14(1):117-127

Varda, D. M. , Forgette, R., Banks, D. and Contractor, N. (2009). Social Network Methodology in the Study of Disasters: Issues and Insights Prompted by Post-Katrina Research From the issue entitled "Hurricane Katrina / Disaster Demography" Population Research and Policy Review, 28(1): 11-29.

15