What Matters Most Among Human Factors to Comply With Organization's Information Security Policy

M. Arif

Shaheed Zulfiquar Ali Bhutto Institute of Science & Technology (SZABIST), 90 Clifton, Karachi, Pakistan
e-mail: effiarif@gmail.com

Abstract

An organization's success or failure in achieving or maintaining its competitive edge mostly depends on its Human Resource (HR). In a striking semblance! organizations both public and corporate around the world are awakening to this reality that security of their information that consists of data basis developed over years of learning as well as research and development, which are critical to their uniqueness may be lost in fraction of time due no one else's doing but their own very HR. Recently more trust was being placed in technology rather than human elements to ensure Information Security (IS), however, happenings over the time have turned the balance as more than 75 % cases reported around the world Pahnila et al. (2007) have been attributed to human factors like, *Security Culture*, *Awareness*, *Training*, *Threat perception* and *Reinforcement*. An empirical study employing both quantitative and qualitative research has been performed to validate the proposed Conceptual Framework based on above human factors deemed important for achieving willingness of the IT users to comply with organizations' Information Security Policies (ISPs). Findings confirm viability of conceptual framework as well as statistical model used. Organization's *Security Culture* emerges as leading human factor contributing to the overall IT security of an organization followed by *Awareness* and *Training.* Findings can be generalized for other geographical regions especially which have resemblance in terms of development, culture and literacy as of Karachi cosmopolitan city of Pakistan.

Keyword

Human Factors, Information security (IS), Information Security Policies (ISPs), Willingness to Comply, Reinforcement, Threat Perception, Theory of Reasoned Actions (TRAs)

1. Introduction

Protection through Human beings has proved highly undependable than the technical/technological approaches Rasmussen (1982). This fact poses a great challenge for the management to establish that what is important to influence the employee's behavior to make them compliant to organizations' security policies. Trade-offs may be noticed with regards to user's work, and social norms. Interaction with organizations' culture and colleagues at work may also influence the understanding of an individual. Every organization expects its employees to safeguard its information and take appropriate actions and initiatives to protect its tangible and intangible assets. Employees are expected to take routine actions like

locking the computer, changing the password frequently, being aware of online threats, using licensed software, taking care of company assets and promptly reporting Information Security (IS) incidents.

Reportedly, between 2001 and 2003 about 75% organizations experienced security breaches of their information, Pahnila et al. (2007). Surprisingly most of the breaches were attributable to company employees due their improper IS behavior. At the same time other human factors e.g *organization culture*, *awareness*, *risk perception*, *training* and *reinforcement* are considered to have strong influence on one's ability to comply with laid down Information Security Policies (ISPs)/regulations and acquire related knowledge. This has generated a discussion among professionals and the academia to dig out causes and come up with remedial measures; with an aim to arrest the situation. Studies in this regard have generally focused on the interplay between human factors and need to comply organization's ISP; same is the core subject of this research study.

2. Problem Description

The study of various research works reveals that these have generally discussed involvement and interplay of human factors and need to comply with organizations' ISPs. However, almost none have tried to prioritize the human factors vis-à-vis the willingness to comply organizational information security policy (OICP), so that remedial/protective measures could be brought to bear against counterproductive human factors with a directed and focused attention to address the problem right at its root cause.

2.1. Study Objectives

The main objectives of the paper are:

- To establish relationship between human factors; *Awareness, Training, Risk perception, Reinforcement* and *Organization culture.*
- Examine the strength of relationship between human factors and an individual's willingness to comply with organizations' Information Security Policies.

2.2. Research Questions

In the light of foregoing discussion following research questions emerge:

- Are the human factors like *Awareness, Training, Risk perception, Reinforcement and* organization's *culture* related to *willingness to comply* with organizations' ISPs?
- What matters most among the aforementioned human factors to achieve willingness to comply with organizational ISPs?
- What possible actions could be instrumental in polishing/grooming the human factors that matter to comply with organizational ISPs?

3. Human Factors

Policies, awareness programs and training in tandem with technology are employed to protect organizations' information to keep them secure and to avoid disclosure to unauthorized entities. Information security encompasses a broad area which deals with IS management as well as data, computer, electronic gadgets and network security. A laid down policy plays a vital role in the security/protection of data. The user interaction/interfaces with security systems have been rationalized and simplified by human factor experts, according to Stanton et al. (2005). Many companies world over are dependent upon IT systems to establish their databases, communications and financial transactions. As the wide use of electronic devices has become more vulnerable to intrusions, therefore, information loss, theft and web page defacing have gained prominence, Stanton et al. (2005). Dhillon and Backhouse (2001) have brought to light that the experts of IS field have been mostly focused on technical aspect of the problem, whereas, socio cultural and human aspect remained neglected. Trend in recent times has shifted to cultural aspects as well (OECD, 2002).

3.1. Culture

Organization culture that evolves over time plays an important role to shape the attitudes, intentions and motivations of individuals' actions towards IS, (Johnson & Goetz, 2007). The organizational culture acts like a personality of that organization Robbins (2001) and connects together all members, Kreitner and Kinicki (1995), Hellriegel et al. (1998) and Robbins (2001) claim that security culture of any organization evolves based on top level vision and the employees' behavior. To shape up security culture, awareness should sink deep at all organizational levels; educating the employees about the value of protecting information, explaining associated risks and strategic effects that loss of information could cause, (Johnson & Goetz, 2007).

The IS attitude of people forms contours of IS culture just as the strong organizational culture moulds the employees, according to Matins (2002), Martins and Elogg (2002), Robbins et al. (2003) and Hellriegel et al. (1998) culture of an organization consists of combined values, behaviors, attitudes, beliefs, and knowledge possessed by the subjects and the stakeholders as well as their involvement with the systems and processes of the organization.

3.2. Awareness

User involvement is expected to improve the IS knowledge. According to Pahnila et al. (2007), careless employees not mindful of organizations' IS are the main source of hazard. Albreshtsen (2007) shows that mostly employees have low awareness as they think that their contribution has no significant effect on the organization's IT security. They lack that necessary knowledge to be ascertained that in what way actions taken by them intentionally or un-intentionally, support or hinder the implementation of organizations' ISPs; in spite of being fully motivated, loyal and

committed to the mission of the organization. Kajava et al. (2007), explain that even the top and middle management lacked full understanding regarding information security. This ultimately hinders their ability to take prudent decisions to enhance organization wide security level. It is therefore, deduced that raising security awareness is equally important both for the top management and people at the operational level. Top management needs to assume leading role to breed and nurture security culture of the organization.

3.3. Training

Awareness is strongly associated with training. The awareness program actually sets foundation for the information security training program. Barman (2002) is perfectly right in saying that awareness and training go hand in hand. Understanding of policies needs serious consideration and to accentuate it further, all stake holders need to be thoroughly trained and apprised of the vitality of their roles. According to Whitman (2008), in view of the huge challenge of implementing ISPs, at the earlier stages it is important to constantly keep the policies alive in the employees mind.

3.4. Risk Perception

The organizational and cultural factors are considered important/relevant to develop an understanding about the risk behavior of employees. According to Beck's (1992) risky society characteristics and Risk prone information systems have an unclear correlation. In the light of this fact, macro-sociological factors further affect the understanding of risk perception behavior (Albreshtsen, 2007). Hone and Eloff (2002) state that any ISP should be framed keeping in mind the organizational culture so that they complement each other and help in sharpening the risk perceptions. (Aytes & Connolly, 2004) in their study about risky behavior found that there was a significant gap between the respondents self perception and committed risky behavior. They further suggested that risks occur seldom but their consequences are mostly negative.

(Aytes & Connnolly, 2004) claim that risk behavior of employees helps explaining their attitude and level of knowledge. Literature on the subject also brings to the fore that risky attitude that remains unpunished may prevail especially if safeguards are not vey potent, Slovic (2000). The information sources, like training, media, friends, policies and personal experience influence a user's perception of threats, awareness and related consequences. User's develop perceptions of system robustness, belief system etc, influence displayed safe behavior, which brings about either favorable or unfavorable outcomes.

3.5. Reinforcement

Buss and Salerno (1984) have suggested in "Common Sense and Computer Security", what measures managers can adopt as matter of reinforcement to ensure the integrity of information systems. Rather than complex and expensive technological measures, auditing and control help detecting incidents of security

breaches at an early stage. Stanton et al. (2005) claim that in order to promote security agenda of the company employees should be motivated and equipped with relevant knowledge. Recently the system administrators, out of their practical experience have professed that installing patches, updating software, training and awareness campaigns are not just sufficient. (Lund & Aaro, 2004) have argued that consolidated measures including awareness campaigns, education, technical/physical initiatives, rewards, legislation and enforcement measures positively influence risk behavior of employees.

3.6. Information Security Policy (ISP)

According to Hone and Elf (2002) most important security measure is having a laid down information security policy (ISP). Managerial policies according to Buss and Salerno (1984) are proving much more successful than purely technical measures. Whitman and Mattord (2009), state that chalking out of an ISP is a basic and fundamental step to secure a company against internal or external attacks. As ISP encompasses, stringent protection and risk free handling of information/data contained and transported between IT systems, it's but fundamental to ensure effective denial measures, Straub (1990). Policy statements prove to be a pulse of managerial intentions as well as emphasize need that employees should remain focused on IS, Wood (1995). Due non availability of instrument of policy, the direction is lost while managerial role and support shall become questionable, Kapp et al. (2009). Generally policy making is considered a technical issue and its enterprise wide importance is not realized, Knapp et al, (2009). Framing and sponsoring ISP should become a stepping stone of corporate governance (Damianides, 2005). Von Solms and Von Sols (2004) have expressed; failure to realize that ISP is the corporate governance responsibility amounts to an act of serious management negligence.

3.7. Motivation

Rogers and Prentice-Dunn (1997), state that intentions are the best measure of one's protective motives. Intentions lead to set of motives having bearing on one's behavior Ajzen (1991). Reward system also complements the motivation, Pierce (2002). By training and enhancing awareness as well as explaining possible threats/negative consequences involved, organizations gain compliance to ISPs. On the contrary, a study by Parker (2002) reveals that users having little training might feel comfortable protecting themselves against viruses attacks as well as data losses. Negative consequences might not influence users' motivation but it certainly affects the company especially if the effects are strategic in nature, (Aytes & Connolly, 2004).

3.8. Willingness to Comply ISPs

Pahnila et al. (2007) have investigated factors that help explaining compliance to ISPs. They have recognized relevant factors and have also tested how these affect users' ability to comply policy to deduce what contributes most. Intentions to adhere

to policy/regulation are rooted in *the theory of reasoned action* (TRA), Fishbein and Ajzen (1975). Attitudes resulting from stimuli, lead to negative as well as positive responses and intent to follow the motives, Ajzen (1991). According to TRA, higher is the intent to commit to certain behavior, higher is the likelihood that it will be performed, Pahnial et al. (2007). Rogers and Prentice Dunn (1997), claim that intention is most relevant measure to map motivation. Direct path from intention to compliance with ISPs is significant, meaning thereby that intention to use any form of measures correlates with the actual use, Venkatsh et al. (2003)

4. Conceptual Framework

In view of the literature research, the conceptual frame work that evolves has been manifested in (Fig-1). Human factors like *Security Culture, Awareness, Training, Risk perception* and *Reinforcement* emerge as *independent variables* and *Willingness of an individual* to comply ISPs of organization emerges as *dependent variable*, which embodies elements of, Theory of Reasoned Action (TRA), *Intention, Attitude* and *motivation* of an IT user.

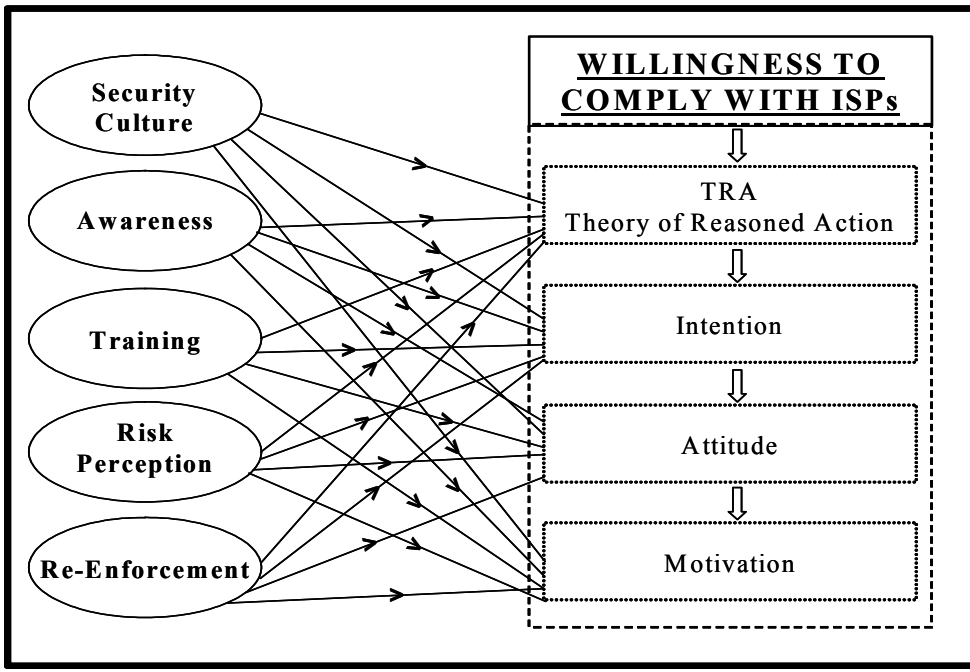

Figure 1: Conceptual Framework

5. Methodology

The conceptual frame work (Fig-1) was taken as model for statistical testing. A sample of 150 was taken comprising participants mostly from middle management

and operational level both from Corporate and Public sector. A written questionnaire prepared on the likert scale was used for survey, 12 questionnaires were discarded due incomplete submission and finally 138 respondents' (*N*, 138) data was used for statistical model testing using SPSS. The participation of top level management was minimal and their solicitation was difficult due high commitment and involved hierarchies. Participation of the female group was also minimal due to their less numbers employed in Pakistan, especially at middle management level. The objective of the statistical analysis conducted using SPSS computer based software was to find answers to the following hypothesis:

5.1. Hypotheses

Following hypotheses were constructed to test intra independent variable correlation as well as independent and dependent variable correlation. To test intensity of relationship between ship testing of independent and dependent variables multiple regression technique was used:

> Hypothesis-I "*A mutual correlation exists amongst all independent variables of the model i.e. Organizations' culture, Awareness, Training, Risk perception and Reinforcement*"
>
> Hypothesis- II "*A strong correlation exists between all independent and dependent variable i.e. Willingness to Comply ISPs*"
>
> Hypothesis–III "Culture*, Awareness, Training, Risk perception* and *Reinforcement* are fairly accurate predictor of *Willingness to Comply I*SPs"

To gain an insight about other intangibles involved in the study i.e. motivation, individual intentions, attitudes and TRAs; in depth interviews were conducted with various levels of management.

6. Findings

The results/findings generated mostly through statistical tests using SPSS and qualitative analysis are reported in the ensuing paragraphs.

6.1. Reliability

As a first step reliability of the questionnaire i.e. testing tool inclusive of all constructs (18 items, 6 constructs of 3 questions each) was tested which was found good and reliable; as the value of (*Cronbach,s Alpha = .724).*

6.2. Response Mapping

Responses of the participants are summarized in *Box Plots* at (Fig-2). Generally responses in respect of all variables are *normally distributed* and *kurtosis/Skewness* is within limit except for "*Security Culture*" where the median is at third *quartile* and

left skewed. It implies that in terms of "*Security Culture*" responses are mostly on the highest side of agreeableness and in order of priority it takes the highest value among other human factors and is followed by, *Awareness*, *Training* and *Risk perception*.

Box Plots results are further complemented by the descriptive statistics. *Security Culture*, (M= 4.1, SD =.527) clearly emerging as the leading variable, whereas, *Reinforcement* (M= 3.9, SD= .591) emerges as the lagging Variable. So it is deduced that the *Security Culture* is the most influential human factor contributing to the willingness of a user to comply with ISPs.

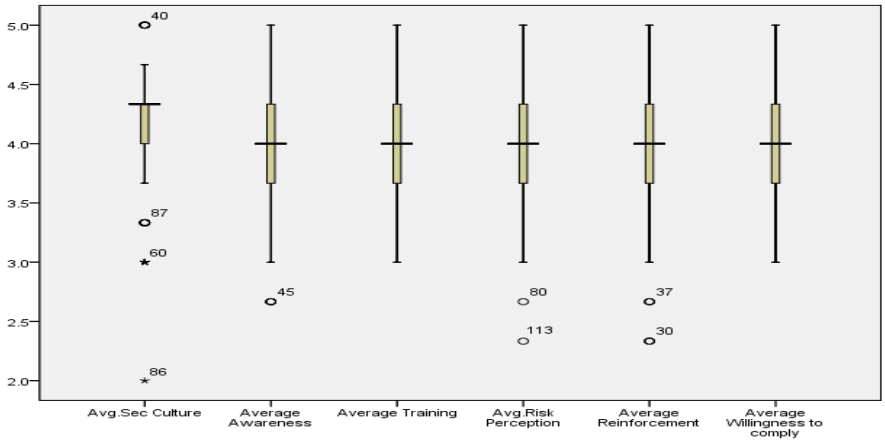

Figure 2: Response Measurement

6.3. Correlation

Results *of Pearson Correlation* test (Table 1) show that there is significant correlation among all the independent variables, concurrently these all are also significantly correlated with dependent variable i.e. *Willingness to Comply* ISPs. Highest correlation 42.4% exist between "*Awareness*" and "*Willingness to comply*" and it is minimum 19.8 % between "Risk perception" and "*Willingness to comply*" however, it is also significant at .05 level of significance. Hence, Hypothesis-I & Hypothesis- II are confirmed and accepted.

		Avg.Sec Culture	Average Awareness	Average Training	Avg.Risk Perception	Average Reinforcement	Average Willingness to comply
Avg.Sec Culture	Pearson Correlation	1	.328**	.231**	.336**	.338**	.398**
Average Awareness	Pearson Correlation	.328**	1	.218*	.207*	.293**	.424**
Average Training	Pearson Correlation	.231**	.218*	1	.113	.351**	.383**
Avg.Risk Perception	Pearson Correlation	.336**	.207*	.113	1	.115	.198*
Average Reinforcement	Pearson Correlation	.338**	.293**	.351**	.115	1	.282**
Average Willingness to comply	Pearson Correlation	.398**	.424**	.383**	.198*	.282**	1

Table 1: Pearson Correlation Table

6.4. Inter Variable Relationship

Multiple Regression Test has been used to confirm and find intensity of relationship among Independent and Dependent variables. Value of (R Square = .321) shows that all the independent variables in unison explain 32.1% of Variance in Dependent Variable *'Willingness to compl'*, whereas, about 68% remains unexplained or there are certain other factors involved like, Loyalty, equity and motivation which need further research. Test of ANOVA further confirms significant relationship among independent and dependent variables. Table of regression coefficients (Table- 2) shows that slopes "β1s" of none of the variables are zero or negative; hence, Hypothesis –III is accepted and positivity of slopes of multiple regression equation confirms positive relationship among all the Independent and Dependents variable, '*Willingness to comply ISP'*.

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95% Confidence Interval for B		Correlations			Collinearity Statistics	
		B	Std. Error	Beta			Lower Bound	Upper Bound	Zero order	Partial	Part	Tolerance	VIF
1	(Constant)	.895	.438		2.041	.043	.028	1.762					
	Avg.Sec Culture	.217	.079	.227	2.747	.007	.061	.374	.398	.233	.197	.755	1.325
	Average Awareness	.255	.072	.278	3.542	.001	.112	.397	.424	.295	.254	.837	1.195
	Average Training	.265	.081	.255	3.289	.001	.106	.424	.383	.275	.236	.853	1.172
	Avg.Risk Perception	.030	.072	.032	.421	.674	-.112	.173	.198	.037	.030	.875	1.142
	Average Reinforcement	.027	.069	.031	.387	.700	-.110	.164	.282	.034	.028	.784	1.276

Table 2: Table of Coefficients

7. Conclusion

In the light of both quantitative and qualitative analysis, the study concludes with good degree of confidence that, *Security culture, Awareness, Training, Risk perception* and *Reinforcement* are important human factors to achieve employee's *willingness* to abide by an organizations' *information security policies* (ISPs); as these have a positive mutual correlation as well as strong predictive relationship with, '*Willingness to comply organizations' ISP'* as matter of priority, organizations' *Security Culture* takes the fore most importance followed by *Awareness* and *Training*. Interestingly '*Risk perception'* emerges being least important Human factor as it is subjective in nature and varies from person to person; however, during in depth interviews it was fairly established that individuals who have suffered a breach of security intentionally or inadvertently generally have high Risk Perception which helps in achieving their willingness to comply ISPs.

As the sample for this study comprised public and corporate organizations situated in the city of Karachi of Pakistan; findings are, therefore, considered more applicable to the same environment, however, as the sample included Multi National Organizations as well; it is, therefore, concluded with fair degree of confidence that results can be generalized for other geographical regions especially, having semblance in terms of development, culture and literacy as of Pakistan.

8. Further Scope for Research

As the statistical model used for this study explains only 32.2 % of the Variance in *Compliance to organizations' Information Security Policies (ISPs,)* which means there are certain other contributory factors like *loyalty, integrity, equity* and *patriotisms* etc*,* which call for further research in this domain.

9. References

Albreshtsen, E. (2007). A qualitative study of users' view of information security. Computers & Security, 26(4), 267-289.

Ajzen, I. (1991). *The Theory of Planned Behavior*. Organizational Bheavior and Human Decision Processes, 50(2), 179-211.

Aytes, K. & Connolly, T. (2004). Computer Security and Risky Computing Practices: A rational choice perspective. *Journal of Organizational and end User Computing*, 16(3), 20-38.

Barman, S. (2002). Writing information security policies. Computer & Security, 28(7), 493-508.

Beck, U (1992). *Risk society: towards a new modernity.* London: SAGE.

Buss M. D. J. & Salerno L. M. (1984). Common sense and computer security. *Harvard Business Review*. 62(2), 112-121.

Cameron, J. & Pierce, W. (2002). *Rewards and intrinsic motivation.* Westport, Conn: Bergin & Garvey.

Damianides, M. (2005). Sarbanes-Oxley and IT governance. New guidance on IT control and compliance. Information Systems Management, 22 (1), 77-85.

Dhillon, G, & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal,* 11 (2), 127-153.

Fishbein, M. & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research.* Reading, Mass: Addison-Wesley.

Hellriegel, D. & Slocum Jr. J. W. & Woodman, R. W. (1998) *Organizational Behavior* (8th edition). Cincinnatio, Ohio: South-Western College Publishing.

HÖne, K. & Eloff J.H.P. (2002). Information security policy – what do international standards say? *Computers & Security,* 21(5), 402-409

Johnson, M. E. & Goetz, E. (2007). Embedding information security into the organization. *Managing organizational security,* 5 (3).

Kajava, J. & Anttila, J. & Varonen, R. & Savola, R. & Ronings, J. (2007) *Senior Executives Commitment to Information Security – from Motivation to Responsibility*. Berlin: Springer.

Kreitne, R. & Kinicki, A. (1995): *Organizational behavior.* Chicago: IRWIN Inc.

Knapp, K. J. & Morris, R. F. J. & Marshall, T. E. & Byrd, T. A. (2009) Information security policy: An organizational-level process model. *Computer & Security* 28 (7), 493-508.

Lund, J. & AarØ, L.E. (2004): Accident prevention. Presentation of a model placing emphasis on human, structural and cultural factors, *Safety Science,* 42(4) 271-324.

Martins, A. & Eloff JHP. (2002). Information security culture IFIP/SEC2002. In: Security in the information society. Boston: Kluwer Academic.

OECD (2002). OECD guidelines for the security of information systems and networks: towards a culture of security. Paris: OECD.

Pahnila, S. & Siponen, M. & Mahmood, A. (2007). *Employees' behavior towards IS Security Policy compliance: An Empirical Study.* Boston: Springer, 232.

Parker, D. (2002). Motivating the Workforce to Support Seucrity Objectives: A Long-Term View. CISSP, RedSiren Technologies, Inc.

Rasmussen J. (1982). Human Errors. A taxonomy for describing human malfunction in industrial installations. *Journal of Occupational accidents.* 4 (2-2), 311-333.

Robbins. S. (2001). Organizational behaviour (9th ed.) New Jersey: Prentice Hall.

Rogers, R. W. & Prentice_dunn, S. (1997). Protection motivation theory, in D. S. Gochman (Ed), Handbook of helath behavior research In: Personal and social determinants, New York, NY, Plenum Press, pp. 133-132.

Slovic P. (2000). *The perception of risk.* London: Earhscan publications ltd.

Straub, D. W. (1990) effective IS Security: An empirical study. *Information systems research,* 1(3), 255-276.

Venkatesh, V. & Morris, M. G. & Davis, G. B. & Davis, F. D. (2003): User acceptance of information technology: Towards a unified view, *MIS Quarterly*, 27(3), 425-478.

Whitman M. E. (2008). Security Policy: from design to maintenance. In: Straub DW, Goodman S., Baskerville R. L., editors. Information security: policy, processes, and practices. *Advances in management information systems,* 11. Armonk, N. Y: M. E. Sharpe.

Whitman, M. E. & Mattord, H. J. (2009). Principles of information security (3rd edition). Massachusetts: Thomson Course Technology.

Wood, C. C. (1995). Writing Infosec. Policies. Computers & Security, 14(8), 667-74.