Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2010 Proceedings

Americas Conference on Information Systems (AMCIS)

8-2010

The influence of human factors on vulnerability to information security breaches

Antonio Carlos G. Maçada
Federal University of Rio Grande do Sul, acgmacada@ea.ufrgs.br

Edimara M. Luciano
Pontifical Catholic University of Rio Grande do Sul, eluciano@pucrs.br

The influence of human factors on vulnerability to information security breaches

Edimara M. Luciano
Pontifical Catholic University of Rio Grande do Sul
e-luciano@pucrs.br

M. Adam Mahmood
University of Texas at El Paso
mmahmood@utep.edu

Antonio Carlos G. Maçada
Federal University of Rio Grande do Sul
acgmacada@ea.ufrgs.br

ABSTRACT

Within the context of information security (InfSec), human aspects have been receiving particular attention in research studies and business practices because of the fundamental role of the users. The objective of this research-in-progress is to develop a theoretical model of how human factors such as behavior with InfSec, familiarity with policies and procedures, awareness, organizational environment, and work conditions, contribute to InfSec breaches. The proposed model will be applied through interviews with CIO, multiple case studies and a survey of information system users in some South American countries and the USA. The sample will consist of end users of integrated web information systems (IS) in large organizations. An instrument will be designed and validated using qualitative and multivariate techniques. This research is intended to contribute towards identifying and managing the impact of human aspects on InfSec breaches.

Keywords

Information Security, human aspects, vulnerability, breaches

INTRODUCTION

Organizations are paying increased attention to InfSec mainly because “the damage due to computer security incidents is becoming higher and higher” (Ng, Kankanhalli and Xu, 2009). In time of intense competition among companies, the protection of information assets is paramount. This should allow companies to avoid financial, image or competitive advantage damages (Liginlal, Sim and Khansa, 2009). However, protecting companies from InfSec attacks has been a challenge. In 1997-1999 CSI surveys, 37-50% of the organizations were victims of InfSec breaches. Despite of the fact that losses have been dropping significantly for the last five consecutive years (CSI, 2008), InfSec is still a concern. As there has also to be considered trust and image losses, not only the financial losses.

Due to infusion of more procedures and logical or physical devices within the information environment, no system can be completely secure (Straub and Welke, 1998). In this context of relative complexity, keeping IT environment safe demands a more complete understanding of the phenomenon, which requires broadening InfSec far beyond the technical aspects. The studies on economics by Anderson and Moore (2006) and Huang, Hu, Behara (2008), on human factors by Ng, Kankanhalli and Xu (2009) and Liginlal, Sim and Khansa (2009), and social aspects by Dhillon and Backhouse (2001) and Dourish and Anderson (2006) confirm this point.

Even technology is important to maintain safe the IT environment, “organizational and human factors also play a crucial role in achieving Information security” (Dutta and Roy, 2008). A lot of breaches are unintentionally caused by users or employees (Alder, 2006), by accident or unwittingly (Ransbotham and Mitra, 2009) by negligence with the procedures (Shaw et al., 2009) or, sometimes, intentionally or knowingly. According to the 2001 Information Security Industry Survey, of all the security breaches perpetrated by employees of organizations, 48% were accidental (Vroom and von Solms, 2004).

Training and awareness are frequently used as tools to improve the human component in InfSec (D’Arcy, Hovav and Galletta, 2009). Probably, awareness is enough for some users, but not for all. For example, ignorance of the consequences of acts, negligence regarding procedures and stress or fatigue can influence the behavior of InfSec and, consequently, the exposure to breaches (Lacey, 2009). In their research, Acquisti and Grossklags (2005) mention that when they asked people about isolated pieces of personal information, the people were not highly concerned if the information was connected to their identifiers or not.

In this context, the objective of this research-in-progress is to develop a theoretical model that will help us understand how human factors can contribute to InfSec breaches. These factors are behavior with InfSec, familiarity with policies and procedures, awareness, organizational environment and work conditions. The research will provide a number of hypotheses based on this model. The importance of the present research-in-progress is to identify and validate human factors that affect InfSec.

The manuscript is structured in the following manner: the next section provides a literature review that describes the constructs used in the present research. This is followed by a description of the research model and the corresponding hypotheses, as well as the methodological aspects. The manuscript concludes by providing a description of method and future research studies and implications for these studies.

LITERATURE REVIEW

A number of authors have affirmed that InfSec depends on human factors. Dutta and Roy (2008) comment that InfSec has been understood mainly as a technical subject, and that "only more recently has it been recognized that InfSec involves a complex interaction between technical, organizational and behavioral factors". Alagar (1986), in his research into data security problems, argued that security is a human problem and concern because human decision and intervention are significant in InfSec. Trcek et al. (2007) mention that the alone technology cannot provide appropriate levels of safety of the information.

Vroom and Von Solms (2004) state that employee behavior is crucial to any organization. Ng, Kankanhalli and Xu (2009) point out that technological control are certainly necessary in assuring InfSec but this security also depends on the individual's security behavior. There are only a few research studies on InfSec behavior of computer users and how this behavior can be modified to practice security countermeasures. Trcek et al. (2007) suggested that human behavior and organization-related issues are usually intertwined in InfSec policies. The authors state that "it has become evident during recent years that technology alone will not and cannot provide adequate security of information systems."

Dutta and Roy (2008) developed a model for interaction between technical and behavioral security factors, and their impact on the business value of an organization's IT infrastructure. The model "captures delays associated with perception of security risk, the mechanics of user compliance and the mechanics of risk mitigation achieved by investments in security technology and user training".

Goodhue and Straub (1991) stated that individual characteristics have a positive impact on satisfactoriness of security measures. The authors further state that when the users are aware of the potential damages that may be caused to their IS they may feel good about implementing InfSec. The authors also mention that better knowledge about information technology can contribute to the avoidance of security breaches. This is because the user can perceive threats more easily.

The following sections discuss the major theoretical dimensions involved in this research, which are users' behavior, familiarity with InfSec aspects, awareness, organizational environment and work conditions.

Users' behavior

Behavior, in the InfSec context, can be understood as actions in relation to InfSec and the manner in which these actions are taken. The behavior of a person is strongly influenced by two aspects. The first is the principles, values, convictions and believes of the person. The second is the environment, such as the organizational culture, the colleagues' opinion and the organizational values. The result of behavior in InfSec can have an impact on recommendations made regarding policies and procedures.

According to Ng, Kankanhalli and Xu (2009), the success of InfSec "depends on the effective behavior of users". The authors developed a model to study user' computer security behavior using a model used in healthcare. The constructs used are perceived susceptibility, perceived benefits, perceived cues to action, general security orientation, self-efficacy and perceived severity which also influences other constructs. Results showed that perceived susceptibility, perceived benefits, and self-efficacy are determinants of related security behavior.

Stanton et al. (2004) explored some of the antecedents surrounding the practices of InfSec by end users. The study shows relations between end-user security behavior and a combination of situational factors (such as organizational type) and personal factors (such as income level and job role). The results revealed that organization type, job role, job satisfaction, and organizational commitment each showed relations to some key security behaviors of end users.

Vroom and von Solms (2004) developed a research with the objective of exploring the potential problems concerning attempts to audit employee behavior. The conclusions of the papers show that this is extremely difficult, especially because the individuals react differently in each situation, depending on their personalities and factors that influence them. Therefore, it is important to understand the employees' behavior and their reasons for it. To move forward in this direction, the authors provide a model to understand the interaction between the organizational culture and behavior. Based on this model, the individual behavior is influenced by the organizational culture and by the group (in an organizational context).

Familiarity with information security aspects

Familiarity with InfSec can be understood as the level of the users' knowledge in relation to InfSec. This knowledge may include little technical aspects or only general knowledge about Information Technology, for instance, having enough knowledge to avoid trusting e-mails with an attractive content but bad intentions. This familiarity avoids that the user acts thoughtlessly and consequently compromises the InfSec.

In their study about behavior of the employee in relation to InfSec, Vroom and von Solms (2004) mention that is mandatory that the employees contribute and take on their responsibility in the process. Shared knowledge about InfSec, according to the authors, is very important because it can contribute towards a change in individual behavior "and eventually in the organization as a whole". This change, according to authors, occurs "slowly but surely".

Shaw et al. (2009), in their study about the impact of information richness on the effectiveness of InfSec awareness training, used the term competence to represent familiarity with InfSec, to create or consolidate a culture and values about InfSec. According to the authors, several security risks are associated with knowledge, such as technical skills and casual computing, the latter being a probable indication of low knowledge.

However, knowledge can be used to attack an information system. Ransbotham and Mitra (2009) mention that many interviewees described the evolution of an incident, starting with exploratory attempts and using the knowledge obtained from these attempts to invade the IS. Shaw et al. (2009) identified the same aspect. The fact that employees have computer skills can be an important barrier for InfSec awareness.

An additional concern in InfSec is social engineering. This term, in the InfSec field, refers to a set of techniques used to obtain important information from and about people or organizations. The goal is obtaining some kind of benefit, such as irregular accesses to systems or places (Winkler, 1995). Most of the times, the capacity these people have to persuade is very significant. Therefore it is vital for employees to know about InfSec and technology in order to avoid being victims of bad intentions.

Awareness

Awareness has been pointed to by several authors as fundamental for the effectiveness of actions intended to enhance InfSec, because, despite the efforts of organizations with the policies, procedures and mechanisms intended to improve InfSec, if the users don't collaborate, nothing will happen.

Awareness, in InfSec, can be understood as the effort that the organization makes with the objective of ensuring and increasing the results of the actions related to the security. In this sense, it has been used to reflect awareness of users about their role in security information (Siponen, 2000).

In general, awareness can be enhanced through training. According to Kruger and Kearney (2006), awareness contributes to creating a positive InfSec culture. This culture is important to ensure actions in accordance with the InfSec policies. An appropriate level of awareness can be a prerequisite for adequate security protection (Goodhue and Straub, 1991).

In their study, Shaw et al. (2009) identified three levels of security awareness: perception, comprehension and projection. Perception is a sense and detects potential security risks within the business environment, allowing an understanding of the presence or awareness of a threat. Comprehension is the knowhow to perceive facts from multiple sources and correctly interpret them. The third level, prevention, is when the end users can use the ability to project or predict future situational events, and this shows that users "have the highest level of understanding of their surroundings".

Awareness is an important action in efforts aimed at providing InfSec. But it is difficult, because it involves a human component and behavioral change. According to Lacey (2009), "changing attitude is much harder". The active participation of employees involved in InfSec is important because they feel they participate in forming policies and procedures, which can contribute towards the observance of such policies.

Organizational environment

Wulff, Bergman and Sverke (2009) mention that job satisfaction has a significant influence on mental ability, and in professional and academic achievement. This satisfaction, according to Goodhue and Straub (1991), can be distinguished in job satisfaction. In this sense, the individual characteristics are an important aspect of a good employer – employee relationship, but insufficient to ensure continued care regarding InfSec procedures.

Chan, Woon and Kankanhalli (2005) explored the influence of the organizational environment on the InfSec system, and concluded that management practices, supervisory practices, and coworker's socialization are positively related to employees' perception of InfSec climate in the organization. In this sense, perception of security climate and self-efficacy had positive impacts on compliant behavior relative to InfSec.

The organizational culture is another important aspect in InfSec, according to Chang and Lin (2007). The authors examined the influence of organization culture on the effectiveness of implementing InfSec management, and concluded that the culture is conducive to InfSec practices and extremely important for organizations because the human dimension of InfSec cannot totally be solved by technical and management measures.

Vroom and von Solms (2004) cite that timing and supervisor's mood influence the evaluation of the employee's performance, especially about shortage, true assessment and unreliability. This influence impacts on many of aspects in this relationship, because the employee reacts to positive or negative stimulus, and the relationship with the managers can create a sense of contribution towards company goals.

When the work environment is positive, it is easier for the employees to understand their role in the complex system of InfSec, avoiding collaboration with invading parties by accident or unwittingly, or due to the negligence with the procedures (Shaw et al., 2009). The most important consequence of a positive environment is that it creates a feeling of belonging to organizational principles and objectives.

An organization with a positive climate can possibly influence the behavior and commitment of employees (Chan, Woon and Kankanhalli, 2005). In the same sense, if there is a good relationship among the employees and between them and the managers, it can contribute towards InfSec, especially with a conscientious behavior about InfSec. This can happen because the employee feel more linked with the company, and this can generate more positive feelings and to take care over the activities.

Work conditions

Kelloway et al. (2010) comments that when the work conditions are not satisfactory for the employees, these can contribute negatively to work. Failure to follow policies and procedures can be influenced by tiredness or fatigue. When an employee is tired, he may unwittingly disregard some InfSec recommendations. Ligindal, Sim and Khansa (2009) identified in their study that mistakes in the information processing stage constitute most cases of human error related to privacy breach incidents. Corfitsen (2003) explains the relationship between tiredness and traffic accidents, mainly because the lack of attention and delay in actions involved in traffic.

Work pressure can influence the acceleration of the work pace, generating a decrease in concentration and increasing stress and anxiety (Mikkelsen, 2002). This feeling can affect the performance of tasks (Bozionelos, 2001). In InfSec, this can result in inattention when handling private information during one's own work or when in contact with colleagues, clients and suppliers.

In the same sense, if an employee is forced to work beyond the regular time, he or she is likely to be psychologically exhausted (Dulebohn, 2009). This will decrease the intrinsic motivation to work and work effort will consequently decrease. Low motivation is a result of many situations in a company, such as lack of recognition, an unchallenging work environment, inadequate salary or unsatisfactory conditions to exercise a professional judgment. The effect of this is a loss of identification with an organization, and a consequent lack of care with all recommendations, including those involving InfSec.

In this sense, negative feelings associated with inadequate work conditions, such as stress, low vitality, anxiety, discouragement, passivity and disinterest, among others, can bring negative consequences to the organization's InfSec plans.

THE MODEL

Based on the literature review, the model for this research is according to Figure 1, below. The focus of the model is on the individual, represented by behavior towards InfSec, familiarity with policies/procedures and awareness. However, the employee behavior is influenced by environment and work conditions. Gender and work experience are the moderators. This model intends understand the influence on vulnerability to InfSec breaches, which is the dependent variable.

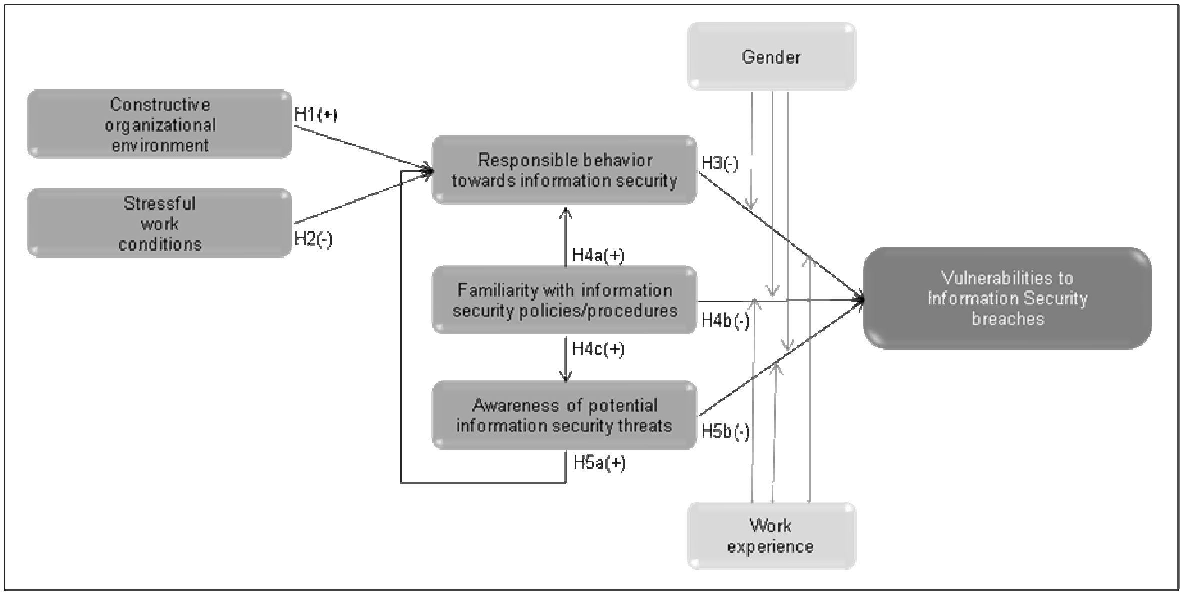
Gender
Constructive organizational environment
H1(+)
Responsible behavior towards information security
H3(-)
Stressful work conditions
H2(-)
H4a(+)
Familiarity with information security policies/procedures
H4b(-)
Vulnerabilities to Information Security breaches
H4c(+)
Awareness of potential information security threats
H5b(-)
H5a(+)
Work experience

Figure 1: Research Model

Based on this model, we propose the following hypotheses:

- H1: Constructive organizational environment will positively impact the responsible behavior towards Information security.
- H2: Stressful work conditions will negatively impact the responsible behavior towards Information security.
- H3: Responsible behavior towards adhering to information security policies and procedures will negatively impact vulnerabilities to information security breaches.
- H4a: Familiarity with information security policies and procedures will positively impact the responsible behavior towards Information security;
- H4b: Familiarity with information security policies and procedures will negatively impact vulnerability to information security breaches;
- H4c: Familiarity with information security policies and procedures will positively impact the awareness of potential information security threats.
- H5a: Awareness of potential information security threats will positively impact the responsible behavior towards Information security;
- H5b: Awareness of potential information security threats will negatively impact vulnerability to information security breaches.

As moderators, were chosen gender and work experience as result of analysis about which are more involved in the research subject.

The research of Kuo, Lin and Hsu (2007) shows that "significant gender differences exist in the subjects' overall self-regulatory efficacy for information privacy". D'Arcy, Hovav and Galletta (2009) used the gender like a moderator in their model, and the results indicate that the gender has direct influence on negative effect on IS misuse intention.

About de work experience, Ma, Johnston and Pearson (2008), in a study with the purpose of develop a framework to InfSec management, conclude that work experience of the professional involved with InfSec is relevant. In this study, the organizations which were moderately sensitive about the InfSec had younger InfSec professionals with less work experience.

The relationship between the hypotheses and the theoretical basis is shown below (Table 1).

Hypotheses **Authors**	**H1**	**H2**	**H3**	**H4a, H4b, H4c**	**H5a, H5b**
Bozionelos (2001)		X			
Cartwright and Holmes (2006)		X			
Chan, Woon and Kankanhalli (2005)	X				
Chang and Lin (2007)	X				
Dulebohn et al. (2009)		X			
Goodhue and Straub (1991)				X	X
Kelloway et al. (2010).		X			
Kruger and Kearney (2006)					X
Lacey (2009)	X				
Lee, Lee and Yoo (2004)			X		
Ligindal, Sim and Khansa (2009)		X			
Mikkelsen (2002)		X			
Ng, Kankanhalli and Xu (2009)			X		
Ransbotham and Mitra (2009)				X	
Shaw et al. (2009)	X		X	X	X
Stanton et al. (2004)			X		
Siponen (2000)					X
Vroom and von Solms (2004)	X	X	X	X	
Winkler (1995)				X	
Wulff, Bergman and Sverke (2009)	X				

Table 1. The relationship among the factors, hypotheses and the theoretical basis is shown below (Table 1).

Additionally to the references exposed in the literature review, we can make use of a couple of theories related to the research topics in order to support the hypotheses. These theories will avail the questionnaire elaboration quite a lot in the second phase of the research.

The Theory of Reasoned Action (TRA) was proposed by Fishbein and Ajzen in 1975. According TRA, people that evaluated a suggested behavior as positive (attitude), and thought that others expected them to perform in a specific way (subjective norm) would result in increased intention to behave as expected (motivation). In InfSec, Lee, Lee and Yoo (2004) and Leonard, Cronan and Kreie (2004) used this theory.

The Theory of Planned Behavior (TPB) proposed by Ajzen in 1985, concerns to the link between attitudes and behavior and can be understood as an extension to the TRA. It has been applied in several studies of IS that explore the relationship among beliefs, attitudes, behavioral intentions and behaviors, such as Leonard, Cronan and Kreie (2004) and Siponen (2000).

The Protection Motivation Theory was created by Rogers in 1975. PMT explains why people engage in harmful practices and offers suggestions to change those behaviors. In InfSec, PMT was used by authors such as Pahnila, Siponen and Mahmood (2007) and Workman, Bommer and Straub (2008).

The General Deterrence Theory (GDT) was originally developed by Ehrlich (1973) and explains why people act in a specific way, even knowing about the sanctions and the consequences of their actions. In InfSec, Straub (1990) and Pahnila, Siponen and Mahmood (2007) used this theory.

METHODOLOGY

As previously explained, this research aims to answer the following questions: what are the determinant variables in the influence of human factors on vulnerability to information security breaches? And, how do they impact such information security breaches? To answer these questions, both qualitative and quantitative techniques will be used, respectively in an exploratory and a confirmatory approach. According to Mayring (2001) it is important to combine qualitative and quantitative methods in the collection and analysis of data since when together they permit more relevant results and conclusions to be reached. The methods that will be used are: interviews with executives (Stake, 1995); multiple case studies (Benbasat et al., 1987); and survey (Koufteros, 1999).

The research will be conducted according the research steps shown below:

a) Qualitative method:

a.1) Interviews will held with CIO executives (from USA and Brazil) with the purpose of examining the applicability of the variables of the model and hypotheses;

a.2) A multiple case study will also be carried out in two leading organizations from different sectors (from USA and Brazil). It is expected that with the case study methodology the factors will be confirmed or otherwise and some variables will be added or removed.

b) Quantitative method:

b.1) The survey will confirm the set of the determinant variables from the model for the influence of human factors on vulnerability to information security breaches. In this step the guidelines provided by Koufteros (1999) will be followed to develop and validate the research instrument. The pilot study will be carried out by applying the questionnaire with experts in information security in USA and Brazil. The final study will consist of applying the questionnaire in Brazilian and American sample enterprises that use intensive information, such as banks, insurance companies and brokers. For the data analysis, a set of statistical tests will be conducted, such as structural equation modeling (SEM).

FUTURE RESEARCH

In order to further our knowledge of information security it is necessary to carry out in-depth studies into the organizational, behavioral and psychological aspects that support the development of robust research models. The next step will be to observe these aspects at the inter-firm level, that is, between firms that share information within the same supply chain.

After the research described in this manuscript, the cultural dimension will be included in the model, specially the national culture studied by Hofstede (1991), as an aspect that have influence on the individual and organizational dimensions. For this, another data collection will be conducted, with people from countries with a clear cultural difference, like as oriental and occidental countries.

REFERENCES

1. Acquisti, A., Grossklags, J. (2005) Privacy and rationality in individual decision making, Economics of Information security, IEE Security and Privacy, 3, 1, 26-33.
2. Alagar, V. S. (1986) A Human Approach to the Technological Challenges in Data Securitv, Computers & Security, 5, 328-335.
3. Alder, G. S., Noel, T. W., Ambrose, M. L. (2006) Clarifying the effects of Internet monitoring on job attitudes: the mediating role of employee trust, Information & Management, 43, 894–903.
4. Anderson, R. and Moore T. (2006) The Economics of Information security, Science, 314, 5799, 610-613.
5. Benbasat, I., Goldstein, D. K., Mead, M. (1987) The case research strategy in studies of information systems, *MIS Quartely*, September, 368-386.
6. Bozionelos, N. (2001) Computer anxiety: relationship with computer experience and prevalence, Computers in Human Behavior, 17, 213-224.
7. Cartwright, S., Holmes, N. (2006) The meaning of work: the challenge of regaining employee engagement and reducing cynicism, Human Resource Management Review, 16, 199–208.

8. Chan, M., Woon, I. and Kankanhalli, A. (2005) Perceptions of information security at the Workplace: Linking information security Climate to Compliant Behavior, Journal of Information Privacy and Security, 1, 3, 18–41.

9. Chang, S. E., Lin, C. (2007) Exploring organizational culture for information security management, Industrial Management & Data Systems, 107, 3, 438-458.

10. Corfitsen, M. T. (2003) Tiredness - a natural explanation to The Grand Rapid "DIP", Accident Analysis and Prevention, 35, 401–406.

11. D'Arcy, J., Hovav, A., Galletta, D. (2009) User awareness of security countermeasures and its impact on Information Systems misuse: a deterrence approach, Information Systems Research, 20, 1, 79-98.

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

13. Dourish, P., Anderson, K. (2006) Collective information practice: exploring privacy and security as social and cultural phenomena, Human-Computer Interaction, 21, 319-342.

14. Dulebohn, J. H., Molloy, J. C., Pichler, S. M., Murray, B. (2009) Employee benefits: literature review and emerging issues, Human Resource Management Review, 19, 86–103.

15. Dutta, A., Roy, R. (2008) Dynamics of organizational Information security, System Dynamics Review, 24, 3, 349-375.

16. Goodhue, D.L., and Straub, D.W. (1991) Security concerns of system users: a study of perceptions of the adequacy of security, Information and Management, 20, 1, 13-27.

17. Hofstede, G. (1991) Cultures and Organizations: software of the mind - Intercultural Cooperation and its Importance for Survival. London: McGraw-Hill.

18. Huang, C. D., Hu Q. and Behara R. S. (2008) An economic analysis of the optimal information security investment in the case of a risk-averse firm, International Journal of Production Economics, 114, 2, 793-804.

19. Kelloway, E. K., Francis, L., Prosser, M., Cameron, J. E. (2010) Counterproductive work behavior as protest. Human Resource Management Review, 20, 1, 18-25.

20. Koufteros, X. (1999) Testing a model of pull production: a paradigm for manufacturing research structural equation modeling, *Journal of Operations Management*, 17, 467-488.

21. Kruger, H. A., Kearney, W. D. (2006) A prototype for assessing information security awareness, Computers & Security, 25, 4, 289-296.

22. Kuo, F., Lin, C. S., Hsu, M. (2007) Assessing gender differences in computer professional's self-regulatory efficacy concerning information privacy practices, Journal of Business Ethics, 73, 145-160.

23. Lacey, D. (2009) Managing the human factor in Information security. Sussex: John Wiley and Sons.

24. Lee, S. M, Lee, S., Yoo, S. (2004) An integrative model of computer abuse based on social control and general deterrence theories, Information & Management, 41, 707–718

25. Leonard, L. N. K., Cronan, T. P., Kreie, J. (2004) What influences IT ethical behavior intentions—planned behavior, reasoned action, perceived importance, or individual characteristics? Information & Management, 42, 143–158

26. Liginlal, D., Sim, I., Khansa, L . (2009) How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management, Computers & Security, 28, 3-4, 1–1 4.

27. Ma, Q., Johnston, A. C., Pearson, J. M. (2008) Information security management objectives and practices: a parsimonious framework, Information Management & Computer Security, 16, 3, 251-270.

28. Mayring, P. (2001) Combination and integration of qualitative and quantitative analysis. Forum: Qualitative and Quantitative Research, 2 (1), http://www.qualitative-research.net/fqs-texte/1-01/1-01mayring-d.htm (Date of Access: December 05, 2009).

29. Mikkelsen, A., Øgaard, T., Lindøe, P. H., Olsen, O. E. (2002) Job characteristics and computer anxiety in the production industry, Computers in Human Behavior, 18, 223–239.

30. Ng, B., Kankanhalli A. and Xu Y. (2009) Studying users' computer security behavior: a health belief perspective, Decision Support Systems, 46, 4, 815-825.

31. Pahnila, S., Siponen, M., Mahmood, A. (2007) Which Factors Explain Employees' Adherence to Information Security Policies? An Empirical Study, Proceedings of the Eleventh Pacific Asia Conference on Information Systems, July 4-6, Auckland, New Zeland.

32. Ransbotham, S., Mitra, S. (2009) Choice and Chance: a conceptual model of paths to information security compromise, Information Systems Research, 20, 1, 121-139.
33. Richardson, R. (2008) CSI Computer Crime & Security Survey.
34. Shaw, R. S., Chen, C. C., Harris, A. L., Huang H. (2009) The impact of information richness on information security awareness training effectiveness, Computers & Education, 52, 92–100.
35. Siponen, M. (2000) A conceptual foundation for organizational information security awareness, Information Management & Computer Security, 8, 1, 31-41.
36. Stake, R. E. (1995) The art of case study research, *Thousand Oaks*, Sage Publications, CA.
37. Stanton, J. M., Mastrangelo, P. R., Stam, K. R. and Jolton, J. (2004) Behavioral Information security: two end user survey studies of motivation and security practices. Proceedings of the Tenth America's Conference on Information Systems, August 6-8, New York, NY, USA.
38. Straub, D. W., Welke, R. J. (1998) Coping with systems risk: Security planning models for management decision making, MIS Quarterly, 22, 4, 441–469.
39. Straub, D.W. (1990) Effective IS Security: An Empirical Study, Information Systems Research, 1, 3, 255-276.
40. Trcek, D., Trobec, R., Pavesic, N., Tasic, J. F. (2007) Information systems security and human behavior, Behavior & Information Technology, 26, 2, 113–118.
41. Vroom, C., von Solms, R. (2004) Towards information security behavioural compliance, Computers & Security, 23, 191-198.
42. Winkler, I. S. (1995) Social Engineering: The Only Real Test of Information Systems Security Plans, Computers & Security, 14, 7.
43. Workman, M. Bommer, W. H., Straub D. (2008) Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior, 24, 2799–2816.
44. Wulff, C., Bergman, L. R., Sverke, M. (2009) General mental ability and satisfaction with school and work: A longitudinal study from ages 13 to 48, Journal of Applied Developmental Psychology, 30, 4, 398-408.