Peer-reviewed academic journal

Innovative Issues and Approaches in Social Sciences

IIASS – VOLUME 5, NUMBER 1, JANUARY 2012

Innovative Issues and Approaches in Social Sciences (IIASS)

Typeset
This journal was typeset in 11 pt. Arial, Italic, Bold, and Bold Italic; The headlines were typeset in 14 pt. Arial, Bold

Abstracting and Indexing services
COBISS, International Political Science Abstracts, CSA Worldwide Political Science Abstracts, CSA Sociological Abstracts, PAIS International.

Publication Data:
SIdip – Slovenian Association for Innovative Political Science
(Slovensko društvo za inovativno politologijo)

Innovative issues and approaches in social sciences, 2012, vol. 5, no. 1
ISSN 1855-0541

Additional information available on: www.iiass.com

SECURITY CULTURE IMPACT ON SECURITY EXCELLENCE IN A COMPANY

Milan Ambrož[1]

Abstract
Awareness and behavior of organizational members is the outcome of the strong, completed and standards supported security culture. A major challenge for the current organization is to promote organizational members to take security responsibly. This paper examines the impact of security culture characteristics on the behavior of organizational members regarding security. My prediction was that the open purpose of the company and its reliability had a significant impact on collective actions regarding security. Additionally, appropriate security culture in a company is the real guarantee for the secure actions of employees. The results of my study support the hypothesis that security culture differentiates between different companies and increases positive behavior of employees towards the security excellence. However, I have found evidence that adaptability and involvement traits of the security culture in our study do not significantly affect the excellence in security behaviour.

I recommend that managers should require employees in the operational security problem solving and continuously and publicly express contemporary and predicted security threats. As a result, reliable preventative actions will come and support the excellence of a company and the quality of the life of all company stakeholders.

Keywords: culture, behaviour, awareness, mission, adaptability, traits, excellence.

Introduction

Safety and security become one of the key business problems for managers of modern organizations. Fraudulent behavior on all management levels and all kinds of trust and security breaches distress and often restrict or destroy business activities. Organization's legitimacy is often under attack. All kinds of different schemes appear that are used to evaluate misuse of company's assets. Such behaviour has to be seriously considered.

[1] Milan Ambrož, PhD is an Associate professor at Faculty of organization studies Novo mesto, Slovenia

Additionally, high pressure of competitive business environment endangers the power of many organizations and a need for a comprehensive security policy, including local and external security are an essential. All kinds of security breaches provoke negative security awareness. They are the basis for the creation of non-integrative view of an organization in the eyes of the employees and customers. Besides, all stakeholders have high expectations regarding security and legitimacy of the business, and security is becoming part of overall efficiency of the organization (Timonen et al 2009). Cumulatively, these factors can have a detrimental effect on a company and its customers and clients. Riughaver et al (2007) and Jiang (2009) prove this statement. They argue that security is a crucial success determining factor in all businesses in the future, especially in high-risk ones.

The aim of this paper is to determine the nature of employees' security behavior in the organization. Relatively little attention has been directed towards how a security culture affects organizational unit's existing security behavior in a management and business environment. I hypothesise that organizational behavior factors contribute to the variety of workplace behavior that adheres to corporate policies and regulations. Further, I suppose that these factors have a positive impact on intentions of company members to behave securely.

Security culture and company excellence

Wiegmann et al. (2002) understand the culture phenomenon in the company through three different perspectives. Sociological perspective highlights heroes, social drama, and rituals manifested in the shared values, norms, and meanings of groups (Deal and Kennedy, 1983; Mearns et al 2003). Anthropological perspective assumes that culture is an emergent property of the organization, generated by its unique history and individual members (Smircich, 1983). In contrast, organizational psychology interpretation defines culture as the values and beliefs that organization members share through symbolic resources such as myths, stories, legends and specialized language (Smircich, 1983). It tends to emphasize its functional role and its impact on the organization productivity (Schein, 1985). Wiegmann (2002) assumes culture as a provider of a conceptual relationship between organizational behavior and management interests. Social identity theory reveals that company members are influenced by the plethora of cultures (Straub et al, 2002).

Security problems are complex and unpredictable. According to Chia, Maynard, and Ruighaver, (2003) security system is one of the systems to be supported by management's beliefs and actions. Leach (2003)

reports that as many as 80 % of serious security failures in Australian companies could be the result of poor security behavior of organizational members. Many organizations still focus exclusively on regulations to submit to minimum standards and whistle-blowing. Such manner obscures the main objectives of integrity (Herath and Rao, 2009). Wagner and Brooke (2007) discuss that the conventional understanding of community that supervises everything has to vanish. Presented empirical evidence leads the development of more proactive and holistic approach to security in a company that makes moral values, individual, shared responsibility, and integrity more precise (Dempsey, 2005). Supervising authority should be delegated to the individual. Chia et al (2003) agrees that the concept of security culture is not fully defined and can be viewed from different points of view generated by different subcultures. Some researchers of organizational culture explain it as a foundation of shared beliefs and assumptions about the way business is done in a company. Security aspect of it reflects the values and beliefs of safety and security. Moreover, security and safety values and beliefs are the basis of security norms and rules that govern the behavior of individuals, groups, or the company (Denison, 2007; Greene and D'Arcy, 2010).

Organizational culture is an emergent and recreated experience as members regularly present and communicate in ways, which seem to them to be natural', clear and unambiguous. Considering this fact, Schlienger and Teufel (2002) argue that security culture is embedded in organizational culture. It is considered to be the general assumption that is changing over time. They argue that it can be designed and changed by the management of an organization. Similar findings were concluded by Bukovec (2009) using different organizational excellence models to implement changes in organizations. In contrast, Detert et al (2000) linked organizational culture to a comprehensive set of values and beliefs that constitute the culture nature' of Total Quality Management. His method consists of eight overarching dimensions that describe the nature of organizational culture. Joo et al (2009) used these dimensions to create a source of security information culture. Da Veiga and Eloff (2010) developed the Information Security Culture Framework. This format is useful in assessing information security in a company.

Starting from this definition, I decided that traits approach is the most suited to my review of security culture. Two of the culture characteristics, collaboration and adaptability, are indicators of flexibility, openness, and responsiveness. They predict growth potential of an organization. The other two characteristics, support and commitment, are indicators of integration, directive, and vision. They are predictors of profitability

(Denison and Mishra, 1995). Security excellence in a company is based on cooperation and flexibility of employees' actions, and their courage and commitment to security and safety. Additionally, security can be maintained by collaborative involvement of organizational members in the security policy and proven adaptability of all stakeholders to the security threats.

Security as a basis of a protective behaviour

Purpose is the most prominent feature of the security culture in an organization. It links structure behavior and goals of the organization. Security purpose consists of formalized information and standardization, certification and evaluation, and it is information about the barrier of concrete and especially information assets. Moreover, it includes organizations member's status, ingenuity and skill in the nature of mental models about security issues. Purpose is the articulation of goals, vision, and strategic direction. Besides, it serves to determine the magnitude of a company and capacity to manage risks and security threats (Pidgeon, 2001). Purpose is aimed to provide security for all stakeholders in the business process, including local, national, and the international. Denison (2007) is convinced that governing a company's purpose clarifies company's goals and projects company's future existence.

Based on the study of organizational culture studies, I identified the following sense of security culture that indicates the relationship of the company to its environment: adaptability to security threats. Lawrence and Lorch (1967) determine the relationship between the extent to which the states of differentiation and integration in the company are compatible to its success. Adaptable organizations do exist and are successful (Denison and Mishra, 1995). They are learning organizations. They continually learn from mistakes, involve risks and do change and growth (Hurst, 1995: 118; Charan, 2004: 161; Coimbra, 2009: 35). Constant pressures to change often negatively affect security. Implementing of reengineering, downsizing, outsourcing and other relief frameworks usually diminishes the sense of security in an organization (Hammer and Champy 1993; Hickok, 1998). Changes in the company certainly modify the security awareness. Culture of fear is often the result of it (Furedi, 2002: 2). Nevertheless, it is necessary for the management of the company to monitor the security threats in internal and external environment and convert them to security regulations and actions. Management has to develop a security policy of network monitoring (Greene and D'Arcy, 2010). In such a manner, management conveys the organizational members and other stakeholders that the company is serious about security (Straub, 1990).

The most valuable asset of the company is employees. They create and manage the company's assets, products, and services. The empirical evidence of Spreitzer (1990), Ambrož (2004), and Denison (2007), has demonstrated that effective organizations provide conditions that empower and improve their employees, and continually strengthen their capacity. Successful organizations provide conditions that enable organizational members. Moreover, empowerment is a process in which an individual enables himself to take effect and management tasks and autonomous decision-making. It is closely linked to the involvement as a work-style characteristic that motivates responsible behaviour. Further, company members feel that they are involved when they can apply to their work and have a strong sense of ownership (Denison, 2007). Organizational members are involved, when they are empowered and can exercise initiative, authority, and ability to manage their own work.

It is particularly noteworthy that organizational members have enough security authority to act and prevent the security breach. This authority includes the right to analyze and to discuss the activities that caused it (Kruger and Kearney, 2006). The initiative to be involved in security issues corresponds to the degree of fulfilled expectations of organizational members. When a contribution of everyone to security in a company is valued, the security will be taken seriously (Weick and Sutcliffe, 2001: 123).

Employees, however, can be a vulnerability to their company's security. If they don't know how to act in a secure manner, they will fail to correspond to security breaches (Hubbard, 2002). Organizations are security operative when they are consistent internally controlled, and fully integrated. Consistent organizations create unique system of governance based on consensus (Denison, 2007). Shuchih et al (2007) analysed the impact of organizational culture characteristics on the effectiveness of security activities in a company. Results of the research show that energy and reliability have a significant impact on information security management. On the other hand, traits cooperation and innovativeness are not significantly associated with it. Only cooperativeness has a significant and negative correlation to confidentiality, which is the essence of security culture. Thomson et al (2006) argues that integration of security into the organizational culture is a fact and is based on the consistent behavior of employees. Security consistency is usually achieved by common agreement on risks and dangers. The quality of the agreement is based on the logical and reasonable doubt in cooperative security activities.

Weill and Ross (2004) argue that open reporting of security problems to the management of a company is successful. It even creates new opportunities for more effective security governance. It could be established through more collaborative opportunities between the business professionals and management and defined technical decisions. Brown and Nasuti (2005) found out that in organizations with the most effective IT governance, IT decisions are shared by all stakeholders. Security consistency is usually achieved by collective agreement on risks and threats, and the quality of the agreement is based on the consistent and reasonable doubt in everyday security activities.

Security excellence and governance

Recently, many disastrous events led to the development proactive and complex concepts in the field of security. One of them is a security culture, which is a complex and challenging project because there are no mutually agreed visible signs, practices and images, values and basic assumptions that define it (Kuusisto and Ilvonen, 2003). Greene and D'Arcy (2010) argue that the quality of a security culture lies in the assumptions and beliefs that drive the organizational members' behaviour. Their research shows that security customs and job satisfaction lead to promote collective security behavior intentions. However, Solms and Solms (2004) and Vroom and Solms (2004) analysis revealed that information system security advocates have suggested that organizations can modify user behavior by cultivating a security culture that promotes security-conscious decision-making and adherence to security policy. For security culture, in particular, and in a functional sense, it is believed to be a significant predictor of security performance, which impacts the overall performance of the organization (Cox and Flin 1998: 189; Javidan, 2004). The level of security performance in the company varies and is dependent upon the extent to which the values promote it (Wiegmann et al., 2002: 5). If the core values and norms about the security are committed, employees internalize them. Moreover, they reinforce the notion of individual and collective security. This is the point where performance is embedded reflecting core beliefs, which are based on need, feasibility and effectiveness of controls.

These conclusions and reports findings led us to the proposition that the security culture fosters security responsible behavior of employees:

H1: The security culture positively impacts the security excellence of the company.

Methodology

Sample

Respondents in our research were from Slovenian public, logistics and one manufacturing company. We deployed 180 questionnaires, and 157 were returned and used in the analysis. The response rate was 95%. Participants completed questionnaire containing questions about the security culture and its impact on security behavior of employees. Participants administered the questionnaires freely and anonymously. It is reasonable to assume that organizational members have been exposed to security issues in their organization, because their organizations emphasized the importance of incorporating security behavior to all business activities. Table 1 below summarizes the characteristics of the respondents and their organizations.

Table 1: Sample description data

Variable	Features	Structure	%
Gender	men	100	64 %
	women	57	36 %
Age	average age	39. 25	
	range of age in years	21-64	
Education	elementary	2	1. 28%
	school	35	22. 30%
	high school	30	19. 11%
	college	30	19. 11%
	faculty	57	36. 30%
	master	3	1. 91%
Organization	public sector	67	42. 67%
	industry	17	10. 82%
	logistics	73	46. 50%

Instrument

Talking to employees about the security is a difficult task. They avoid such interviews because they think that some personal information would be revealed to the unauthorized persons. So we turned to the questionnaire that has been administered in different organizations from a business and social sphere. By questioning the employees, we gained some insight as to how they integrated their security awareness cognitions in the patterns of change behaviours. The means for our analysis based on the organizational culture traits developed by Denison (1990, 2007). As argued by Denison et al (2006) confirming the traits of organizational culture requires the use of a questionnaire, which contents the five groups of questions that we believe constitute a full understanding of cultural traits and security behavior: (a) mission (b)

adaptability (c) involvement (d) security excellence, and (e) awareness. Participants fulfilled questionnaires using Likert-type scale ranging from (1 = totally agree) to (totally disagree = 5).

Analysis of results

My research has produced some significant findings, which we hope will contribute to the literature in this area of inquiry. The empirical findings are discussed below.

Factor analysis

Table 2 shows the results of subjecting the material to principal component factor analysis with Varimax normalized as a technique of rotation to establish content validity of the a-priori dimensions. Specifying five factors were found to have produced the most interpretable results and explained 52.98 % of the total variance.

Table 2: Security culture characteristics

Security culture characteristics	Mission	Adaptability	Involvement	Excellence	Awareness	Mean	Std	Cronbach's alpha
The processes in our organization are transparent enough and can be predicted.	0.62	0.01	0.23	0.12	0.07	3.31	1.07	
Organizational members in our organization report hidden mistakes which could trigger severe consequences.	0.50	0.12	0.05	0.24	0.22	3.42	1.12	
In the organization, we often thoroughly analyse problems to understand them better.	0.64	-0.02	0.23	0.33	0.12	3.39	1.02	
Organizational members in the organization are stimulated to share different opinions.	0.73	0.01	0.17	0.25	0.02	3.55	0.98	
We value organizational members in the company that are skeptical and don't believe everything that is told to them.	0.49	-0.32	-0.24	0.1	0.23	3.11	1.05	0.90
There is a person in the company that has an authority and the power to support our decisions to solve suddenly emerging problems.	0.58	0.20	0.21	0.28	0.11	3.58	1.12	
Organizational members in our organization know the activities in the neighboring processes exceptionally well.	0.69	-0.06	0.20	0.12	0.16	3.21	1.11	
Managers in our organization continuously monitor workload and employ extra sources to reduce it when it is necessary.	0.66	0.07	0.18	0.24	0.13	3.08	1.21	
The members in our organization respect differences in personalities.	0.64	0.05	-0.02	0.29	0.19	3.63	1.03	
Knowledge is in our organization is more appreciated that status in the company hierarchy.	0,67	0.03	-0.03	0.17	0.13	3.41	1.15	
Professional help in our organization is available when we are confronted with the problem that cannot be solved.	0.63	0.10	0.16	0.43	0.11	3.63	0.98	
Working tasks in our organization follow substantial and timely progression.	-0.12	0.40	0.07	0.30	0.22	3.54	1.01	
All procedures of the working process in an organization can be directly observed.	0.27	0.74	0.04	0.02	0.04	2.95	1.15	0.58
Working processes in our organization can be stopped. Products can be warehoused and services held and yet there is no harm done.	0.04	0.60	-0.04	-0.05	-0.19	2.29	1.17	
There are various ways to produce our products or services in our organization. Planning of production or services is changing.	0.02	0.75	-0.14	-0.17	-0.08	2.60	1.16	

continue Security culture characteristics	Mission	Adaptability	Involvement	Excellence	Awareness	Mean	Std	Cronbach's alpha
Employees in our company do not have enough authority to act when unpredictable events occur or when our company is in danger.	-0.34	-0.08	-0.48	0.04	-0.02	2.81	1.17	
When an unexpected event occurs in our company, we usually pay attention to the causes.	-0.08	0.16	-0.76	-0.15	0.02	2.73	1.12	
When activities do not follow the plan in our organization, employees rarely try to find out what is the cause of it.	-0.17	-0.01	-0.73	-0.22	-0.12	2.71	1.05	0.72
To verify whether hypotheses can be accepted, is not the common procedure in our organization.	-0,06	-0.09	-0.71	-0.14	-0.19	2.78	1.14	
Employees in our company rarely discuss concrete security problems.	-0.36	0.25	-0.45	0.02	-0.00	3.04	1.17	
It is common in our company that we fulfill all expectations of our customers.	0.06	0.15	0.08	0.70	0.29	3.94	0.96	
It is known that our company respects ethical business.	0.32	0.09	0.04	0.64	0.07	3.92	0.91	
Our company has clearly defined security politics.	0.26	-0.28	0.03	0.68	0.11	3.93	0.89	
It is evident for our company that it has a clearly defined security rules that are active and operational.	0.32	-0.21	0.05	0.70	0.15	3.83	0.95	
It is common in our company that employees are capable of taking care of the safety of the organization.	0.34	-0.02	0.13	0.53	0.26	3.92	0.86	0.83
It is common for our company that employees actively, flexibly, and effectively secure the company information.	0.34	0.08	0. 1	0.70	0.13	3.79	1.01	
It is known that our company business is secure and stable.	0.32	-0.05	0.13	0.72	0.23	3.93	0.89	
It is obvious, what are the contents of safe and secure behaviour in organization.	0.34	-0.15	0.08	0.67	0.23	3.74	0.99	
It happens in our company that some security and safety measures are abandoned for the sake of customer satisfaction with the company.	-0.02	-0.04	-0.21	-0.56	0.32	2.34	1.21	
We spend a lot of time in our organization considering how our activities might harm our company, stakeholders, partners, and customers.	0.21	-0.09	0.11	0.24	0.61	3.16	1.09	
There is a firm agreement in our organization of what cannot go wrong.	0.27	-0.04	0.25	0.26	0.57	3.58	1.04	
There is a firm agreement in our organization what could go wrong.	0.24	0.01	0.12	0.16	0.66	3.49	1.00	0.71
Organizational members in our company do not believe everything what they see and hear.	0.02	-0.18	-0.13	-0.02	0.58	3.35	1.11	
There is an enormous effort in our organization to produce quality work.	0.21	0.09	0.13	0.21	0.55	4.15	0.81	

The hidden dimensions showing in Table 3 extracted by principal components factor analysis demonstrated adequate reliability of dimensions. It is ranged from satisfactory to excellent, except for the dimension Adaptability to security threats.

Table 3: Cronbach's Alfa reliability of factors

Security mission of the organization	α = .90
Adaptability to security threats	α = .58
Involvement of employees	α = .72
Security excellence	α = .83
Security awareness	α = .71

The first factor, 'Security mission of the organization', explained the 30.18% of variance. It is obvious that the sharing of different opinions and information about business processes could enhance the security awareness of employees.

The second factor 'Adaptability to security threats' explained the 6.82% of variance. When there are different ways to provide products or services and the company is growth oriented, it is flexible enough to adapt to security threats. Additionally, when all procedures of working processes are directly monitored, they can be stopped and continuously improved. Damage from future security threats can be avoided.

The third factor 'Involvement of employees', explained 5.86% of variance and deals with unexpected events that occur in the organization. Participants in the survey pay attention to the activities that caused unexpected events. When activities do not correspond to the plan, participants in the analysis always try to find out what is the purpose of it. It is the normal procedure in the institution to verify whether the hypotheses about the causes that produced deviation from the system are authorized.

The fourth factor, 'Security excellence', explained 5.59% of variance, encompassed many aspects behaviour that strengthens the security of a company and fulfils the expectations of company's customers. It shows that a company has clearly defined security rules that are actively followed. Additionally, it shows that organizational members engagingly and effectively protect the data in an organization. Companies participating in the study create well defined security system with defined goals what to protect, and ethical standards how to do it.

The last, fifth factor, 'Awareness', explained 4.54% of variance. It attempts to respond to the question: "What could and what could not go

wrong in the organization, and to the considerations how the activities of the company's members can damage the organization?" The factor confirms that behavior change is partly based on the reasonable doubt of the members in everything what they see and now. Participants in the study believe that consistency is the result of their tremendous power to produce quality work.

To see if the factor analysis for our example from Table 2 is just, we ran The Kaiser-Meyer-Olkin (KMO) degree of sampling adequacy. A Kaiser-Meyer-Olkin provides an indication (between 0 and 1) of the proportion of variation among the variables that might be accepted variance. This variance can be seen as a measure of underlying or potential common factors. A Kaiser-Meyer-Olkin near 1 indicates the obvious choice to use factor analysis, and KMO less than 0.5 indicates that factor analysis is a not proper procedure to reducing the number of variables. According to Kaiser Index, the results of our example in Table 4 show that factors research is commendable (KMO =. 869).

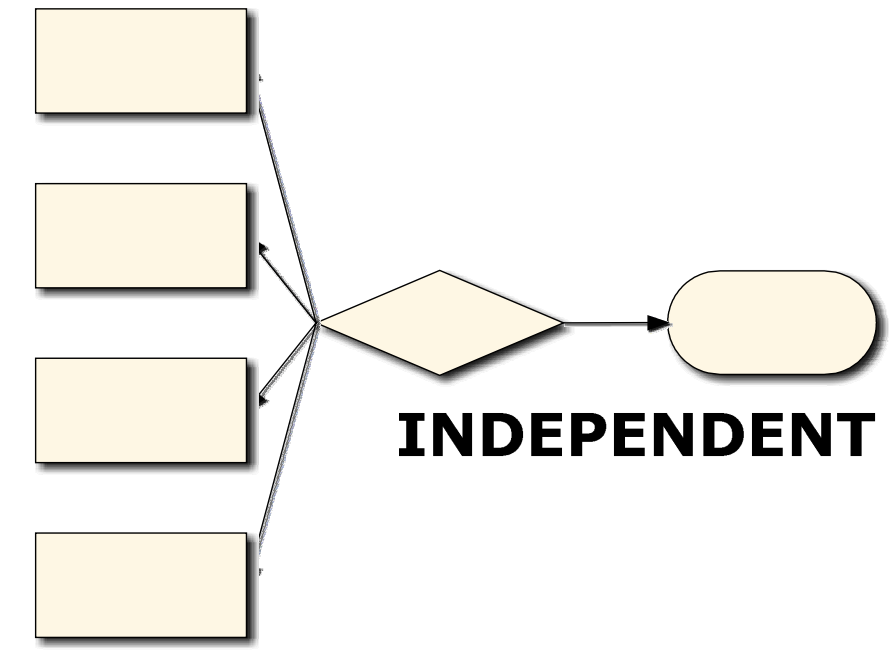
Table 4: The results of the sample adequacy in the study

Kaiser-Meyer-Olkin Measure of sampling Adequacy	.869
Bartlett's test of Sphericity	2649.935
df	630
Significance	.000

Regression analysis

In order to verify the validity of impact of security culture on company employees' submissive behavior, this study uses the Weighted Least Squares Multiple Regression analysis as its research methodology. The objective of regression analysis was to determine the extent to which security values can predict the strength cooperative behavior of organizational members. In order to investigate this effect, we constructed the model presented in Figure1.

Figure 1: Model of security cooperativeness



Compliant behaviour of employees was used as a dependent variable in the model. Security culture traits named: (1) mission, (2) adaptability, (3) involvement, and (4) consistency, were used as independent variables in the regression model. 'Company type' was added as weighted variable.

Table 5: Model summary

Model	R	R^2	Adjusted R^2	Standard error of estimate	Significance of F change	Durbin-Watson
Security excellence	.725	.526	.513	4.33	.000	1.53

As indicated in a Table 5, regression model explains 51, 3% of the variance. Traits: 'Mission' and 'Awareness' show statistically significant relationships with dependent variable. Traits 'Adaptability' and 'Involvement' dropped from the regression calculation because their contribution to security behavior is non-significant. Traits 'Mission' and 'Awareness' were found to be reasonably and positively correlated to the consent of organizational members to act according to security standards. These results are consistent with previous findings from

Greene and D'Arcy (2010) who predicted that security culture, job satisfaction, and perceived organizational funds have a positive impact on organizations IS security. Empirical evidence of partial coefficients' relationship with dependent variable presented in Table 5 shows that security 'Mission' explains the largest amount of variance (52 %). It is followed by 'Awareness' that explains (34 %) of variance. Findings of the analysis show that target and awareness oriented security impact the cooperative actions of the company employees in the field of security.

Table 6: Partial coefficients in the model

		Unstandardized Coefficients		Standardized Coefficients		Significance	Correlations			Collinearity Statistics	
							Zero-order	Partial	Part	Tolerance	VIF
Model		B	Std. Error	Beta	t						
Culture traits	(Constant)	1.431	.319		4.486	.000***					
	Mission	.442	.058	.526	7.580	.000***	.676	.524	.423	.647	1.544
	Adaptability	-.033	.045	-.042	-.741	.460	-.010	-.060	-.041	.975	1.026
	Involvement	-.017	.049	-.022	-.352	.725	-.339	-.029	-.020	.797	1.255
	Awareness	.254	.057	.289	4.433	.000***	,. 61	.338	.248	.734	1.362

Notes: *p < 0.05; **p < 0.01; ***p < 0.001.
Entries are significant standardized regression coefficients

Discussion

In this paper, I empirically tested the model on the benefit security values on security cooperative behavior of organizational members. Empirical results suggest that purpose in the form of a mission and security awareness significantly explain the guarantee of compliance behavior. The results also provide some evidence that these factors or traits are moderated by weighted variable 'Organization type'. Relationship between security culture traits and collective behavior of company employees supports my assumption of the impact of security culture on cooperative behaviour of employees.

However, as noted, extant research has conceptualized security culture as basic characteristics for commitment to excellence. My study contributes to the content validity of the security culture by transforming four organizational culture characteristics based on Denison et al (2006) principles, to the characteristics of a security culture. The examination of the security excellence advances our understanding of the factors that enable company employees' behaviour towards the secure business environment. This behaviour is demonstrated as an excellent information security.

However, the results regarding the adaptability and involvement security characteristics were not as expected. Further research is needed to confirm that security culture develops excellent security behaviour. Based on the extant literature I expected that adaptability and involvement of employees would predict it, but there was no significant relationship. Most likely explanation is that purpose accompanied by regular security governance is the prevailing factor in determining security compliance of employees resulting in security excellence. Systematic review of security threats already involves the setting of a comprehensive security system that is an essential condition for a systematic development of security compliance actions. However, it is appropriate that involvement of employees and consistency of surveillance activities does not knowingly verify agreement actions. Firstly, company management does not include employees in the operational security problem solving process and secondly, security threats are not publicly presented to the employees.

Conclusions

This study has implications for both the research and practice of security in an organization. From a research perspective, this paper offers conceptualization of security culture by adding different views, and the representation of the involvement of the employees in the active solving of security problems. The present study is also one of the few in the security studies that include behavioural variables. For practitioners, the results point to the importance of organizational member commitment to security as drivers of security culture, which in turn contributes to competitiveness of a company. Further, efforts to create a safe and secure environment where organizational members can commit themselves to the core business goals of the organization, would improve the overall quality of life and the quality of interaction with an environment.

Limitations and future research

This study like the others has some limitations that need to be considered when interpreting the results. My research suggests that the relationship between the security culture traits and compliance behavior of organizational members may be contingent on some additional factors. Future studies should assess the impact of culture traits in other companies from different private and public sectors. The methods to determine security culture must be improved by using nonlinear methods for statistical analysis. The measurement tool of security culture has to be supplemented with new items describing adaptability and involvement of company employees in the building of the strong security compliant behaviour.

References

Ambrož, Milan, (2004): Total quality system as a product of the empowered corporate culture. *TQM Magazine,* Vol. 16, No 9, pp.: 93-104.

Brown, William, and Nasuti, Frank (2005): Sarbanes-Oxley and Enterprise Security: IT Governance and what it takes to get the job done. EDPACS, vol. XXXIII, No. 2.

Bukovec, Boris (2009): Integration of various quality control models in organizations, *Innovative Issues and Approaches in Social Sciences*, Vol. 2, No 3, pp.: 37-57.

Charan, Ram (2004): *Profitable growth is everyone's business*. New York, Crown Business.

Chia, Pauline, Maynard, Sean, and Ruighaver, Antonie (2003): *Understanding Organisational Security Culture,* In Hunter, M. G. and Dhanda, K. K. (Eds.) *Information Systems: The Challenges of Theory and Practice*, Information Institute, Las Vegas, USA, pp.: 335 – 365.

Coimbra, Euclides (2009): *Achieving Excellence with Kaizen and Lean Supply chains*. Zug, Kaizen Institute.

Cox, Sue, Flin, Rhona (1998): Safety culture: philosopher's stone or man of straw? *Work and Stress*, Vol 12, No 3, pp.: 189-201.

Da Veiga Alan, Eloff, Jan (2010): A Framework and assessment instrument for Information Security Culture, in Computers & Security, 29(2), 196-207, March 2010.

Deal, Terrence, Kennedy, Alan (1982): *Corporate Cultures: The Rites and Rituals of Corporate Life*, Harmondsworth, and Penguin Books.

Dempsey, Alison (2005): Build an ethical culture before the whistle blows. *Law Now*, Vol. 29, No 9 -10.

Denison, Daniel (2007): Is your company's culture helping or hindering? Diagnosing company culture to build high performance. Available at: http://www.imd.org/research/challenges/TC063-07.cfm.

Denison, Daniel, Mishra, Aneil (1995): Toward a Theory of Organizational Culture and Effectiveness. *Organization science*. Vol. 6, No 2, pp.: 204-223.

Detert, James; Schroeder, Roger; Mauriel, John (2000): Framework For Linking Culture and Improvement Initiatives in Organizations, *The Academy of Management Review*, Vo. 25, No 4, pp.: 850-863.

Furedi, Frank (2002): *The Culture of Fear*. London, Continuum.

Greene, Gwen. D'Arcy, John (2010): Assessing the Impact of Security Culture and the Employee – Organization on IS Security Compliance, Fifth Annual Symposium on Information Assurance [Albany, NY, June 16-17].

Herath, Tejaswini, Rao, Raghav (2009): Protection motivation and deterrence: a framework for security policy compliance in

organisations. *European Journal of Information Systems*. Vol. 18, No 2, pp.: 106-125.

Hubbard, Phil (2003): Fear and loathing at the multiplex: everyday anxiety in the post-industrial city, *Capital & Class*, No 8, pp.: 72.

Hurst, David (1995): *Crisis & Renewal: meeting the Challenge of Organizational Change*. Boston, Harvard Business School Press.

Javidan, Hanges (2004): *Performance orientation*, In: House, R., Hanges, P., Javidan, M., Dorfman, P., and Gupta, V. (Eds), *Culture, Leadership, and Organizations: The GLOBE Study of 62 Societies,* Sage Publications, Thousand Oaks, CA.

Jiang, Xiao (2009): Strategic management for Main Functional Areas in an Organization. *International Journal of Business and management,* Vol. 4, No 2, pp.: 154 -157.

Joo, Soon, Lim; Chang, Shanton; Maynard, Sean; Atif Ahmad (2009): Exploring the Relationship between Organizational Culture and Information Security Culture, *Proceedings of the 7th Australian Information Security Management Conference*.

Kruger, Hennie; Kearney, W.D., (2006): A prototype for assessing information security awareness, *Computers & Security*, Vol. 25, No 42, pp.: 89-296.

Kuusisto, Tuija; Ilvonen, IIlona (2003): *Information Security Culture in Small and Medium size Enterprises.* Frontiers of e-Business Research.

Lawrence, Paul; Lorsch, Jay (1967): Differentiation and Integration in Complex Organizations. *Administrative Science Quarterly*, Vol. 12, No 1, pp.: 1-47.

Leach, John (2003): Improving User Security Behaviour. *Computer & Security,* Vol. 22, No 8, pp.: 685-692.

Mearns, Kathryn; Whitaker, Sean; Flin, Rhona (2003): Safety climate, safety management practice and safety performance in offshore environments. *Safety Science.* Vol. 41, pp.: 641-680.

Pidgeon, Nick (2001): Safety culture: Transferring theory and evidence from the major hazards industries Journal of Cross-Cultural Psychology, pp.: 22, 129-141.

Ruighaver, Antonie; Maynard, Shean; and Chang, Shanton (2007): Organisational security culture: Extending the end-user perspective. *Computers & Security*, Vol. 26, No 1, pp. 56-62.

Schlienger, Thomas; Teufel, Stephanie (2002): Information Security Culture: The Socio-Cultural Dimension in Information Security Management, Proc. Of IFIP TC11 17th International Conference on Information Security (SEC2002), Cairo, Egypt. IFIP Conference Proceedings 214, pp.: 191-202.

Schein, Edgar (1985*): Organizational Culture and Leadership: A Dynamic View*. San Francisco, Jossey-Bass.

Shuchih, Ernest; Chin-Shien, Lin (2007): Exploring organizational culture for information security management, *Industrial Management & Data Systems*, Vo. 107, No 3, pp.: 438 – 458.

Smircich, Linda (*1983*): Concepts of Culture and Organizational Analysis. *Administrative Science Quarterly.* Vol.28, No 3, pp.: 339-358.

Spreitzer, Gretchen (1996): Social structural characteristics of psychological empowerment. Academy of Management Journal, Vol. 39, No 2, pp.: 483-504.

Straub, Detmar; Loch, Karen; Evaristo, Roberto; Karahanna, Elena; Srite, Mark (2002): Toward a Theory-Based Measurement of Culture. Journal of Global Information Management. Jan-March 2002, Vol. 10, No 1, pp.: 13-23.

Timonen, Laura and Luoma-aho, Vilma (2010): Sector-based corporate citizenship. *Business Ethics: A European Review*. Vol. 19, No 1, pp.: 1-13.

Thomson, Kerry Lynn; von Solms, Rossouw; Lynette Louw (2006): Cultivating an organizational information security culture. *Computer Fraud & Security*, Vol. 10, pp. 7-11.

Wagner Andreas; Brooke Carole (2007): Wasting Time: The Mission Impossible with Respect to Technology-Oriented Security Approaches. *The Electronic Journal of Business Research Methods,* Vol.5, No 2, pp. 117 - 124, available online at www.ejbrm.com.[Accessed on 28. July 2011].

Von Solms, Rossouw; and von Solms, Basie (2004): From policies to culture, *Computers& Security*, Vol. 23, No. 4, pp.: 275-279.

Weick, Karl; Sutcliffe, Kathleen (2001): *Managing the Unexpected: Assuring High Performance in an Age of Complexity*. Wiley, Jossey-Bass.

Wiegmann, Douglas; Zhang, Hui; von Thaden, Thierry; Sharma, Gunyan; and Mitchell, Alyssa (2002): A Synthesis of Safety Culture and Safety Climate Research. University of Illinois Aviation Research Lab Technical Report ARL-02-03/FAA-02-2.

Vroom, Cheryl; von Solms, Rossouw (2004): Towards information security behavioural compliance, *Computers & Security*, Vol. 23, No 3, pp.: 191-198.