

The influence of Organizational Citizenship Behavior on Information Security Behaviors

(A Case Study on Meteorological Organization of Iran)

¹Azin Vahidi, ²Saeide kakavand³Mohammad Jafar Tarokh

^{1,2} Department of Industrial Engineering, South Tehran Branch, Islamic Azad University, Tehran, Iran
³ Department of Industrial Engineering, K.N. Toosi University of Technology, Tehran, Iran

ABSTRACT

The purposes of the study were to examine the relationship between organizational citizenship behaviors and information security behaviors. We distributed 120 questionnaires to Meteorological Organization of Iran. The study used SEM and analyzes them using LISREL software package. there are eight secondary hypotheses and one main hypothesis about organizational citizenship behaviors and information security behavior. The results of the research were that information security behaviors can be influenced positively by organizational citizenship behavior.

Keywords: *Organizational Citizenship Behavior, Information Security Behavior, LISREL*

1. INTRODUCTION

Organizational citizenship behavior (OCB) has been the focus of attention from organizational behavior researchers [20,22] show that OCB has an important efficacy on people and organizations and work places. Citizenship behaviors are behaviors which are helpful to the company, yet they are not behaviors considered part of the core elements of the job. Citizenship behaviors are often performed by employees to support the interests of the organization even though they may not directly lead to individual benefits [19]. Organ (1986) shows that behavior is not a requirement of formal job description.

As securing information becomes increasingly more important to the field of organization and management, many companies are seeking more secure methods to protect their organization's personal, private, and financial information. This reaserch for better Organizational citizenship behavior has resulted in organizational concerns over which security methods work best. Traditionally, hardware and software techniques have been posited for information safety. Recently, an emphasis on humanist methods has come to the forefront [12].

We recognized that, there are some items of OCB, which influence on information security behaviors of individuals in organizations. So we test a pilot organization for understanding these behaviors. This article has a major purpose: to determine the existence of a direct link between OCB and Information security behavior.

2. LITERATURE REVIEW

We define behaviour of organizational citizenship as behaviour outside the field of traditional task statements and formal organizational reward systems that in general,

promote the efficient and effective function of the organization[13,33]. The following OCB subscales were defined by Smith, Organ and Near (1983) : altruism (e.g., helps others who have been absent; volunteers for things that are not required; orients new people even though it is not required; helps others who have heavy workloads) and compliance (e.g., punctuality; attendance at work is above the norm; gives advance notice if unable to come to work; does not take extra breaks; does not spend time in idle conversations). OCB was refined by Organ (1988) as the components like: altruism, courtesy, conscientiousness, civic virtue, and sportsmanship. Podsakoff et al. (1990) developed an OCB instrument using Organ's subscales which defined altruism as discretionary behaviours that have the effect of helping a specific other person with an organizationally relevant task or problem and conscientiousness as discretionary behaviours that go well beyond the minimum organizational requirements in the such fields of attendance, obeying rules, and taking breaks. LePine, Erez and Johnson (2002) said that such differences among dimensions are unjustified because they instead reflect a global OCB construct. A new meta analysis of OCB literature found that Organ's (1988) first two subscales (altruism and courtesy) described a single construct; OCB towards individuals (OCB-I) and the last three subscales (conscientiousness, civic virtue, and sportsmanship) described a second construct; OCB towards organizations (OCB-O) [13]. Nevertheless, the Hoffman et al. findings also suggested that current perationalizations of OCB are best viewed as indicators of a general OCB factor Williams and Anderson (1991) first proposed the distinction between the target of the behaviour. A connection between different antecedents (i.e. personal or contextual) and different levels of targets in the organization is permitted by this distinction between types of OCB (i.e. individual/organization as a whole) [26]. Many researchers concur with the Williams and Anderson distinction [3,826] although there is significant



disagreement about the number of significant subscale constructs of OCB-I and OCB-O (see Table 1).

Table1. Summary of Selected OCB Models [12]

	Smith, Organ & Near (1983)	Organ (1988)	Williams Anderson (1991)	Barbuto et al. (2001)	LePine et al. (2002) Hoffman et al. (2007)
OCB-I	Altruism	Altruism Courtesy	OCB-I (7 items)	OCB-I (3 items)	OCB (single construct)
OCB-O	Compliance	Conscientiousness Civic virtue Sportsmanship	OCB-O (6 items)	OCB-O (3 items)	

In information intensive organizations secured management of information has become an important issue. Organizations have been actively using security technologies. Extant research in information security has been focused on the use technology [9].

There are some empirical studies that evaluate organizational security practices and their effectiveness (see table2). However, the respondents are typically IT administrators or top-level managers [7,17,28], and there have been hardly any representation from the end-user community. A recent empirical study [23] evaluating perceptions regarding access controls reports that employees perceive increase security conformity as greater job interference. Most participants of an ICIS 1993 conference panel reported that organizational information security policies are necessary, however, they perceived them to be ineffective [15]. In an empirical study, Frank et al. (1991) found that user knowledge and informal department norms were related with the security-related behavior while the existence of formal policies regarding PC security was not associated with security related behavior. Knapp et al. (2006) security manager opinion study indicates that employee perceptions about security policies are still unclear and varied. In influencing the employee behavior we can draw upon some theory such as: agency theory, Protection Motivation, Social Influence, Facilitating Conditions, Organizational Commitment, Deterrence theory, TRA, TPB, TAM intrinsic motivation, Organizational behavior, Organizational climate, Game theory which has been widely studied in organizational context. Studying in the organization that is our case study, there are One main hypothesis (1) the organizational citizenship behaviors, organizational commitments has a positive relationship with ISB.

And 8 secondary hypotheses:

1. There is a positive relationship between Altruism and OCB
2. There is a positive relationship between Respect, and OCB

3. There is a positive relationship between Conscientiousness and OCB
4. There is a positive relationship between Civil Virtue and OCB
5. There is a positive relationship between Sportmanship and OCB
6. There is a positive relationship between Organizational Obient and OCB
7. There is a positive relationship between Organizational Loyalty and OCB
8. There is a positive relationship between Organizational Participative and OCB

Table2: Summary of Selected ISB reaserch [12]

Title	Related literature with research focus	Theories used/proposed	Core of the literature
Conceptual papers in behavioral security	Poshunnus and von Sothen, Vroom and von Sothen	Components of effective security governance.	Papers with discussion on components of security governance and conceptual perspectives on end-user behaviors.
Mishra and Dhillon and Bachhouse	Socio-organizational or behavioral approach to security.	Theory of anomie	
Strub and Vance	Need for more empirical research using socio-organizational perspectives to develop key principles for the prevention of negative events that will help in the management of information security.	Deterrence theory	
Siponen	Factors affecting/inhaling use in organizations.	TRA, TPB, TAM intrinsic motivation	
Theoharidou et al.	Conceptual foundation for organizational information security.	Deterrence theory	
Abrahamson	Insider threats to information systems and effectiveness of ISO 15404.		
Empirically tested studies in behavioral security	Dixon et al.	Qualitative study of users' view on information security.	Papers with end-user behaviors in variety of contexts such as security tool use, home users, password practices etc.
Anderson	User behavior in using preventative technologies.	Protection motivation, TPB	
Stanton	Security perceptions in organizations - found that end users perceived security practices to be a hindrance to their normal routine.	TPB, TAM, Hofstede's cultural dimensions	
Post	Role of organizational commitment on various security-related behaviors.	Organizational behavior	
Peace et al.	Security perceptions in organizations - found that end users perceived security practices to be a hindrance to their normal routine.	Deterrence theory	
Papers focusing on security policy compliance	Rahimi et al.	Role of threat appraisal, facilitating conditions, and information quality on IS security policy compliance.	Information security policy compliance research is still in early stages. [11] analytically evaluate incentive mechanisms, it remains empirically untested.
Chan et al.	Game theory to evaluate the role of performance incentives in security policy compliance.	Organizational climate	
Gupta and Zhanov	Game theory to evaluate the role of performance incentives in security policy compliance.	Game theory	

3. MATERIALS AND METHODS

In our study we defined 8 items for OCB in our case study in Meteorological Organization: Altruism, Conscientiousness, Civil virtue, Sportsmanship, Organizational Obient, Respect, Organizational Loyalty, Organizational Participative.

The aims of this study are therefore threefold: (1) we want to explore the items of organizational citizenship behaviors in this study; (2) we want to ensure the meaning and character of the organizational citizenship behaviors in this study; (3) want to explore the items of the information security behaviors in this study (4) we want to ensure the meaning and character of the information security (5) we want to examine that the organizational citizenship behaviors influence the information security behaviors positive. The primary research questions to be addressed in this study are as follows: (1) Is there any positive relationship between OCB and ISB? (2) Witch items of OCB have the most influence on ISB?

The data used for this study was collected from an Meteorological Organization in Iran. A survey questionnaire was distributed to employees. A total of 120 surveys were collected, and we don't have any missing data for this study. The participants answered a total of 66 questions on a 7 point Likert-scale, ranging from 1(strongly disagree), to 7(strongly agree. The survey questionnaire was designed to collect information concerning two areas of management constructs: OCB and ISB. We have used the following equation to calculate the sample size,

$$n = \frac{N Z_{\frac{\alpha}{2}}^2 \sigma_x^2}{\epsilon^2 (N - 1) + (Z_{\frac{\alpha}{2}}^2 \sigma_x^2)} \quad (1)$$

- n= the size of the sample
- N=the size of the population =300
- α = the level of error =0.05
- $Z_{\frac{\alpha}{2}}$ = the amount of statistic normal distribution =1.96
- σ_x^2 = the population variance $2x \sigma =9.33$
- ε = the level of confidence=1.3

Cronbach Alpha (1951) was calculated as 0.85, which well above the minimum acceptable limit, 0.70, and we can conclude the results are highly valid. the structural equations were used to study the relationship among different component with factor analysis. The analysis was performed using LISREL software package and SPSS and they are discussed. We used LISREL to precede the factor analysis and reliability and precede CFA of SEM. Let

OCB represents organizational citizenship behavior and IS represents information security behavior.let γ_{ij} be structural coefficients of external variable to internal variable. Therefore, we have the following relationship,

$$IS = \gamma_{11} OCB + \xi_1 \quad (2)$$

In this relation we have IS for Information Security and OCB for Organizational Citizenship Behavior.

4. RESULT AND DISCUSSION

The first step in our survey is to examine the values of t-students and fig1 shows details of our survey.

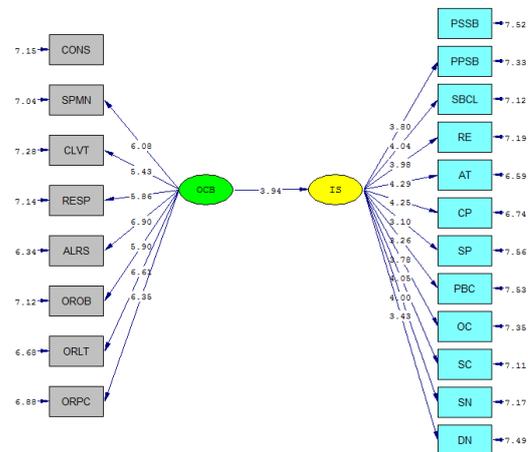


Fig.1, T-student results

The results show that all of t-students are highly valid ($t > 1.96$), which indicates they are meaningful (fig.1).

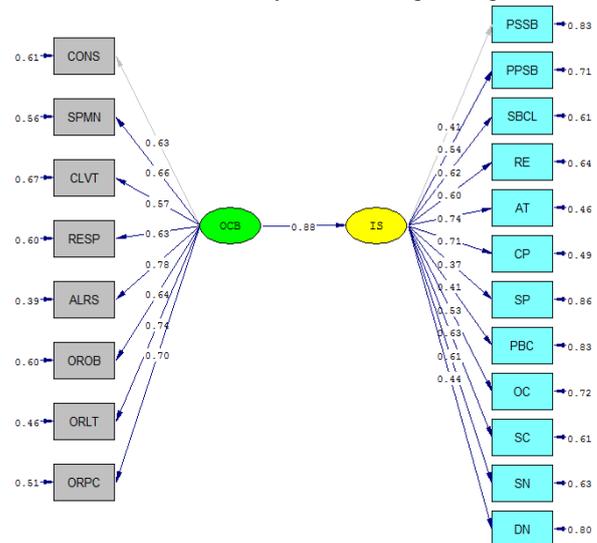


Fig.2, The results of estimated coefficients



Based on the results represented in Fig.2, we have extracted two relationships as follows,

$$IS = 0.88OCB \tag{3}$$

We can show that according two items, t- student and Factor Loading in the output of the software shows us the model has a good validity. (table 3)

Table 3: Validity of modelin with stimate t- student and Factor Loading

SPMN	6.084	0.159
CLVT	5.433	0.200
RESP	5.860	0.171
ALRS	6.898	0.187
OROB	5.903	0.181
ORLT	6.607	0.221
ORPC	6.351	0.208
PPSB	3.802	0.297
SBCL	4.043	0.330
RE	3.982	0.337
AT	4.293	0.292
CP	4.248	0.318
SP	3.100	0.280
PBC	3.265	0.265
OC	3.776	0.298
SC	4.054	0.367
SN	3.996	0.286
DN	3.432	0.190

Table 4 shows the Measurement part of the Model and we estimate the Combined Reliability of the model with following formula,

$$P_c = \frac{(\sum \lambda)^2}{[(\sum \lambda)^2 + \sum(\theta)]}$$

P_c = Combined Reliability

λ = realationship between indices

θ = Error Variance

Table 4: Combined Reliability of variables

No	Latent variables	(P_c)
1	Organizational Citizenship Behavior	0.778
2	Information Security Behavior	0.804

This values shows the highly valid and the model has very good reliability.

For testing the identification problem of the model, it is necessary that the number of independent variables less than the items of Manifest variables of covariance matrix (Long, 1983). As the following we have,

$$t \leq \frac{s}{2} \tag{5}$$

$$s = (9 + q)(p + q + 1) \tag{6}$$

P= Number of x Manifest variables (7)

Q= Number of y Manifest variables (8)

Therefore we have s= 420 and we know that t= 40 (in the model) then we have:

$$t \leq \frac{s}{2} \rightarrow 40 \leq 420 / 2 \rightarrow 40 \leq 210 \tag{9}$$

Therefore we can result that the model is Identification.

Table 5 shows some indices for the Fitting of the model.

Table 5: Fitting indicates of the model

Indices of Fit	Calculated value	validity
RFI	0.931	More than 0.9 is excellent
CFI	0.901	More than 0.9 is excellent
IFI	0.902	More than 0.9 is excellent
NNFI	0.98	More than 0.9 is excellent
NFI	0.926	More than 0.9 is excellent
AGFI	0.923	More than 0.9 is excellent
GFI	0.91	More than 0.9 is excellent
RMSEA	0.07	between 0.05 and 0.08
RMR	0.048	less than 0.05
$\frac{\chi^2}{df}$	2.01	Between 2 and 5

The root mean square error of approximation (RMSEA) is calculated as 0.07, which is relatively a good value for our results. In addition, the goodness of fit index (GFI) and adjusted GFI (AGFI) are 0.91 and 0.923, respectively. This means that our estimations are suitable and very good. We have also considered Normed fit index (NFI), Non-



Normed fit index (NNFI), comparative fit index (CFI), incremental fit index (IFI) and relative fit index (RFI) as 0.926, 0.98, 0.901, 0.902 and 0.931, respectively. These observations clearly validate our results since they are well above 0.9 and it shows that our model has a good fit.

Table 6: Hypotheses

Hypotheses	Coefficient	p-value	t-student	R ²	Result
1	0.391	0.030	6.342	0.609	confirm
2	0.602	0.039	7.138	0.398	confirm
3	0.607	0.039	7.150	0.393	confirm
4	0.669	0.059	7.284	0.331	confirm
5	0.563	0.031	7.036	0.437	confirm
6	0.595	0.043	7.120	0.405	confirm
7	0.459	0.049	6.679	0.541	confirm
8	0.512	0.048	6.881	0.488	confirm

According to the table 6 we show that all of the hypotheses are confirmed. The results show that all of the t values are more than 1.96, p-values has a good validity and coefficient is good.

Main hypothesis: There is a positive relationship between OCB and ISB

According to the LISREL output we can show that p-value is 0.022 which is less than 0.05, t-value is 3.642 which is more than 1.96, R² is 0.767 and all of this values show that the relationship between two variables with coefficient value of 0.876 will be confirmed.

5. CONCLUSION

We have presented an empirical study to measure the relevant impact of different factors such as Altruism, Respect, Conscientiousness, Civil Virtue, Sportmanship, Organizational Obient, Organizational Loyalty, Organizational Participative for OCB indicate and Severity of Penalty, Certainty of Penalty, Security Breach Concern level, Perceived Probability of Security Breach, Organizational commitment, Subjective Norm, Descriptive Norm, attitude, security culture, perceived behavioral control, Response Efficacy for ISB indicate.

Acknowledgment

This study investigated the relationship of Organizational Citizenship Behavior (OCB) and Information Security Behavior (IS) in Meteorological Organization in Iran. The study distributed 120 questionnaires and they were analyzed using LISREL software package. There were one main hypothesis and eight secondary hypotheses

associated with this survey and the results indicated that OCB had strong positive relationship on ISB, accordingly.

REFERENCES

- [1] Albrechtsen, E.(2007). A qualitative study of users' view on information security, *Computers & Security*, 26, 4.
- [2] Anderson, C. (2005). Creating conscientious cybercitizen: an examination of home computer user attitudes and intentions towards security. Presented at Conference on Information Systems Technology (CIST)/INFORMS, San Francisco, California.
- [3] Barbuto, J. Brown, L. Wilhite, M. & Wheeter, D. (2001). Justify the underlying motives of organizational citizenship behavior. A brief study of agricultural co-op workers.
- [4] Chan, M. Woon, I. 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
- [5] Dhillon, G. Backhouse, J. (2001). Current directions in IS security research: towards socioorganizational perspectives. *Information Systems Journal*, 11
- [6] Dhillon, G. Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*, 16,3.
- [7] Dinev, T. Goo, J. Hu, Q. and Nam, K. User Behavior Toward Preventive Technologies Cultural Differences Between the United States and South Korea, *Information Systems Journal*, (Forthcoming).
- [8] Ehrhart, M. G. (2004). Leadership and procedural justice climate as antecedents of unit-level organizational citizenship behavior. *Personnel Psychology*, 57, 61 – 94.
- [9] Fernández-Medina, E. Trujillo, J. Villarroel, R. Piattini, M. (2006). Access control and audit model for the multidimensional modeling of data warehouses. *Decision Support Systems*, 42
- [10] Frank, J. Shamir, B. Briggs, W. (1991). Security-related behavior of PC users in organizations. *Information and Management*, 21, 3
- [11] Gupta, A. Zhdanov, D. (2006). Role of performance incentives in compliance with information security policies, Presented at Conference on Information Systems and Technology. Pittsburgh, PA.
- [12] Herath, T. Rao, H.R. (2009). "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness", *Decision Support Systems*, 47, 154–165



- [13] Hoffman, B.J., Blair, C., Meriac, J., & Woehr, D.J. (2006). Expanding the criterion domain? A meta-analysis of the OCB literature. Paper presented as an All Conference Top Poster at the 21st annual conference of the Society for Industrial and Organizational Psychology, Dallas, TX. This paper was recognized as a finalist for the 2006 John C. Flanagan Award.
- [14] Knapp, K.J. Marshall, T.E. Rainer Jr., R.K. and Ford, F.N. (2006). Managerial Dimensions in Information Security: A Theoretical Model of Organizational Effectiveness. PalmHarbor, Florida and Auburn University, Auburn, Alabama.
- [15] Loch, K. Conger, S. Oz, E. (1998). Ownership, privacy and monitoring in the workplace: a debate on technology and ethics. *Journal of Business Ethics*, 17
- [16] Long, J. S. (1983). Covariance structure model: An introduction to LISREL, Beverly Hills, CA. Sage, P.66.
- [17] Ma, Q. Pearson, J.M. (2005). ISO 17799: "Best practices" in information security management? *Communications of the Association for Information Systems*, 15
- [18] Mishra, G. Dhillon, S. (2006). Information systems security governance research: a behavioral perspective, Presented at 1st Annual Symposium on Information Assurance, Academic Track of 9th Annual NYS Cyber Security Conference, New York, USA.
- [19] Moorman, R. H. and Blakely, G. L. (1992). 'A preliminary report on a new measure of organizational citizenship behavior'. In: *Proceeding of the Annual Meeting of the Southern Management Association*, Valdosta, GA, pp. 185-187.
- [20] Organ, D. W. (1988) "Organizational Citizenship Behavior: The Good Soldier Syndrome". Lexington, MA: Lexington Books, Pahnla, S. Siponen, M. Mahmood, A. (2007). Employees' behavior towards is security policy compliance, Presented at 40th Hawaii International Conference on System Sciences (HICSS 07), , Hawaii, USA.
- [21] Peace, A.G. Galletta, D. Thong, J. (2003). Software piracy in the workplace: a model and empirical test. *Journal of Management Information Systems*, 20, 1
- [22] Podsakoff, P. M., Mackenzie, S. B., Moorman, R.H., and Fetter, R. (1990). "Transformational Leader Behaviors and Their Effects on Followers' Trust in Leader, Satisfaction, and Organizational Citizenship Behavior", *Leadership Quarterly*, 1, 107-42.21.
- [23] Post, G.V. Kagan, A. (2007). Evaluating information security tradeoffs: restricting access can interfere with user tasks. *Computers & Security*, 26, 3
- [24] Posthumus, S. von Solms, R. (2004). A framework for the governance of information security, *Computers & Security*, 23, 8.
- [25] Siponen, M.T. (2000). A conceptual foundation for organizational information security awareness, *Information Management and Computer Security* 8 (1)
- [26] Somech, A & Drach-Zahavy, A. (2007). Strategies for coping with work-family conflict: The distinctive relationships with gender role ideology. *Journal of Occupational Health Psychology*, 12, 1, 1-29.
- [27] Stanton, J.M. Stam, K. Guzman, I. Caldera, C. (2003). Examining the linkages between organizational commitment and information security. Presented at IEEE Systems, Man, and Cybernetics Conference, Washington, DC, USA.
- [28] Straub Jr, D.W. Nance, W.D. (1990). Discovering and disciplining computer abuse in organization, *MIS Quarterly*, 14, 1.
- [29] Straub, D. Collins, R.W. (1990). Key information issues facing managers: software piracy, proprietary databases, and individual rights to privacy, *MIS Quarterly*, 14, 2.
- [30] Theoharidou, M. Kokolakis, S. Karyda, M. Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers and Security*, 24
- [31] Vroblefski, M. Chen, A. Shao, B. Swinarski, M. (2007). Managing user relationships in hierarchies for information system security, *Decision Support Systems* 43
- [32] Vroom, C. von Solms, R. (2004). Towards information security behavioural compliance, *Computers & Security*, 23, 3.
- [33] Williams, L. J., & Anderson, S. E. (1991). Job satisfaction and organizational commitment as predictors of organizational citizenship and in-role behaviors. *Journal of Management*, 17, 3, 601-617.