View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Journal of Telematics and Informatics

Journal of Telematics and Informatics (JTI)
Vol.2, No.1, March 2014, pp. 22~28
ISSN: 2303-3703

Information Security Behavioral Model: Towards Employees' Knowledge and Attitude

Saurabh Mishra, Snehlata, Anjali Srivastava
Indian Institute of Information Technology, Allahabad, India
Email: Saurabhmishraiiita2012@gmail.com, Snehlatasingh361@gmail.com
loginaanjali@gmail.com

Abstract

Information Security has become a significant concern for today's organizations. The internal security threats acts as the most curtail type of security threat within an organization. These internal security threats are a result of poor conduct of security behavior by the employees within an organization. If not deal properly, it may hamper the auditing of organization. Auditing plays an important role in the business environment. Before conducting auditing it is essential to examine the behavioral aspect of the employees. The objective of this paper is to take out this internal threat that acts as a security slack, out of an organization by using a well-structured approach to develop a security behavior model. To validate the proposed model a survey method is used. The survey method measures the knowledge and attitude of an individual employee towards information security to analyze the behavioral security aspect of the employee's. Statistical Analysis of the result of survey indicates that the employees' knowledge and his attitude towards information security derive his behavior towards achieving ultimate organizational goal and thus validates the proposed security model.

Keywords*: Information Security, security model, internal security, Knowledge and Attitude*

1. Introduction

Information Security at the organizational level aims at securing the information asset and other assets of the organization from threats that may exploit the vulnerabilities and get access to the assets of the organization. The various domains of information security in an organization that are often talked about are : Physical (environmental) security , legal regulatory ,investigation & compliance, business continuity and disaster recovery, operations security, cryptography, software development security, Information Security Governance and Risk management , Telecommunication & Network security and Access Control. Although it's known than an employee for an organization is the most important asset to the organization, yet discussing it as a separate domain (BehavioralSecurity) has yet not gained its importance.

This paper discusses about the behavioral security domain, by analyzing the two important aspects of an individual that he/she imparts to the organization: Knowledge and Attitude. It further discusses on how this behavioral security ultimately leads to the organizational security and thus aligns with the organizational goal.

Conducting a performance appraisal of an employee is a task of challenge for an organization. True assessment of performance becomes a mere factor of chance if proper inputs are not taken into consideration. The problem occurs when various factors negatively influence and effect the performance appraisal. Thus the performance appraisal varies depending upon an individual's situational factors. For example, personnel factors of an employee such as his mood, his desires, his fitness in terms of health, his perception, all affect the final outcome. Similarly the personalfactors of the evaluator such as his mood, his dislike for the employee, will affect the final outcome. All these factors at some or the other point becomes a hindrance in evaluating the performance appraisal of an employee and thus influence the accuracy of the measurement.

It can be argued that the problem discussed hear is similar to auditing an employee's behavior. It can be considered as an initial step or a step that needs to be performed just before putting our hands into an information security Audit of an enterprise.

Since all organizations whether profit or nonprofit has employees at the very micro level, and employee is not machinery. Human mind is rational and cannot be taken for granted. Thus working on employees' behavior and getting a unique and ideal model to audit behavioral

Received December 19, 2013; Revised February 7, 2014; Accepted February 26, 2014

security is not a formula based approach and varies depending upon the varying constraints. The best approach that can be considered is the one that fits into a general working environment of any organization, i.e. the organizational structural approach.

2. Research Model

Organizational Division

An organization is a system with several subsystems where people work together in a coordinated manner to achieve the goals of the institution.To obtain synergy, there should be division of labor as well as coordination of activities and efforts [1]. The structure of an organization could take different forms, determined in part by the overall strategy developed to achieve its goals. However at a very granular level an organizational structure can be classified into a number of processes running to in parallel to achieve the ultimate organizational goal. Processes are classified based on a set of activities to be performed together in coordination to achieve required output. Thus there exist various processes in an organization. Each of these processes are controlled and managed by a group leader. Under each leader there exist a number of individual employees.

This implies that there are cascade of goals in an organization that are to be achieved to ultimately get the business level goal that relates to the organizational goal. Thus there are departmental goals that are achieved via number of process level goals at a divisional level. These processes are performed under the supervision of a leader that acts at the regional level. Thus the leader works to attain the team level goal. Within each team there are individuals who work together at individual level to attain the team goal. These individuals work to achieve the individual goal as per the need and task being assigned to them by their leader. Thus in this way connectivity exist at various levels: individual, regional, divisional, business with the ultimate objective of achieving the organizational goal. This structure can be described as follows:

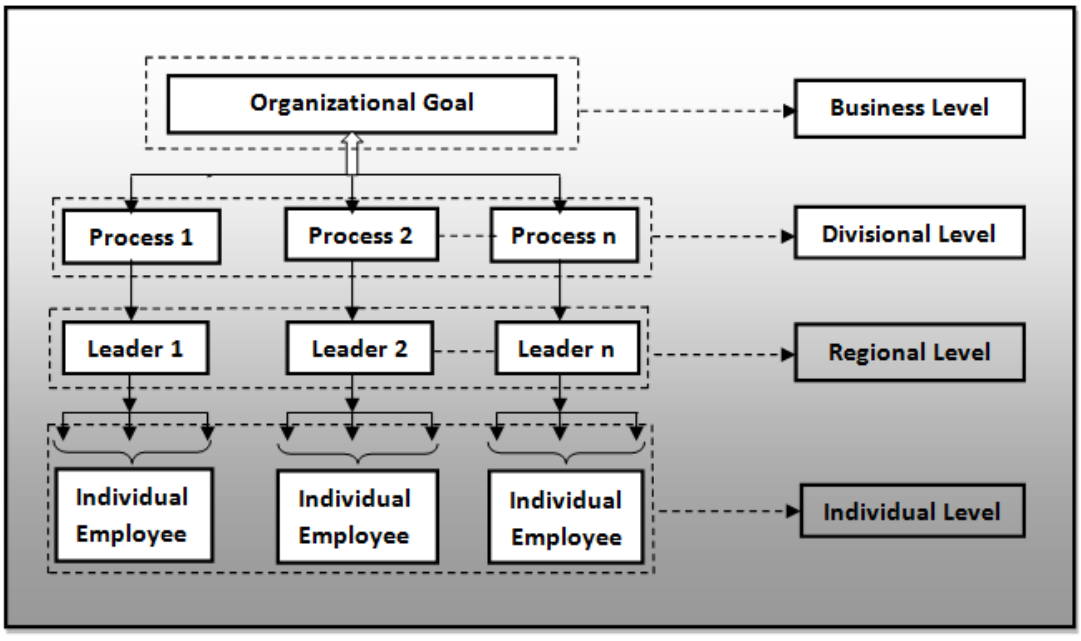

Figure 1. Model for Organizational Structure

Behavioral Security

Individuals' behavior plays a very important role in an organization. To take into consideration an individual's behavior two important factors that are considered are: Attitude and knowledge, Figure 2.

Attitudes denote our positive and negative responses to people, events, and objects and are influenced by the values held by individuals and their sense of right and wrong [1]. Attitude is something that is not developed in a day. Every individual has some inner values and beliefs that they develop with time. As we grow we watch the people around us behaving in a particular way; we are being told to cherish certain things over others that we learn from our teachers and peers. We come to value certain things over other, thus forming our value system. These in turn gives rise to development of our attitudes.

Just as values influence attitudes, attitudes influence behavior [1].

Here we are concerned with the behavioral aspect of attitude because it is behavioral part of attitude that actually governs the end outcome as per the organization model discussed in this paper. It is the behavioral component of attitude that will translate one's desire into actions. Thus behavioral component of attitude falls into two groups:

- An individuals' understanding of what attitude is expected from them in the company.
- An individual's willingness to constrain their attitude to follow the accepted and approved norms.

Knowledge is defined as the facts, information, and skills acquired through experience or education. The knowledge that an individual employee has concerning information security with respect to the organization in which they work is very important. At some or the other level every individual employee in an organization needs to take a security decision. Sometimes these decisions are taken in a non-critical situation where a bit of deviation from the ideal decisions can be tolerated whereas certain decisions need to be taken in a critical or sensitive situation. In such a situation the user has to make an instant decision about what needs to be donein particular circumstances. Such instances where an immediate decision is required by an individual employee, is where the knowledge factor of an individual becomes an important constraint for the end result or outcome. This knowledge factor is attained by one's learning capability as well as ones' past experience that is based on the previous security decisions taken over a period of time.

Here it must be noted that knowledge is too vast and an individual's knowledge may not always lead to a correct security decision for every situation an individual may encounter. However it should, at a minimum be aligned with the organizational policies and procedures, so that information, which is a crucial component of knowledge, is managed securely. Hence an individual cannot avoid making their own security decisions as part of their daily task.

The use of knowledge of an individual in an organization affects discretionary behavior and thus helps to avoid causing offence or revealing confidential information. It also provides an individual the freedom to decide what should be done in a particular situation.

When the attitude and knowledge of an individual employee in an organization combines it gives rise to individual's behavior.

The research model proposes that user knowledge and his attitude together acts as input to an individual's behavior. When such behavioral approach combines it gives rise to a group behavior andreflects an important constraint towards achieving a successful process, Figure 2.

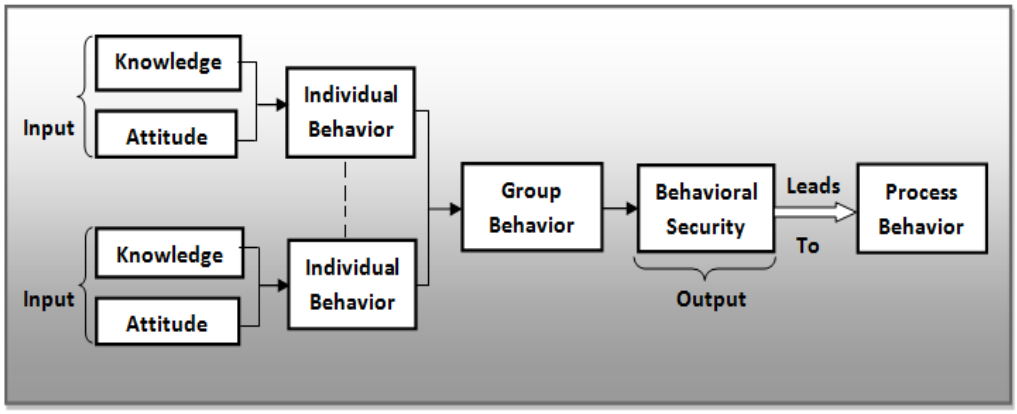

Figure 2. Interaction between Individual Level, Regional Level behavior and Divisional Level behavior

Process level Security

Various individual's behavior at the individual level combines to give rise to process level security. Thus a combination of individual employee's behavior and their leader's behavior at a particular process level is responsible for the completion of a process within an organization.

At a very granular level an individual's behavior towards an organization may appear to be a small thing. But when behavior of a group of individual employees, working together for a specific outcome, is seen, it affects the process they thisgives raise to the process behavior. This process behavior is controlled by a leader. To attain the end level business goal that relates to the organizational goal it is required that the divisional level goals must be attained. This is possible only if the various processes at various divisional levels fulfill their specific requirements and process behaviors are up to mark. Combining these process behaviors gives rise to process level security, when taking into consideration the behavioral aspect of information security, Figure 3.

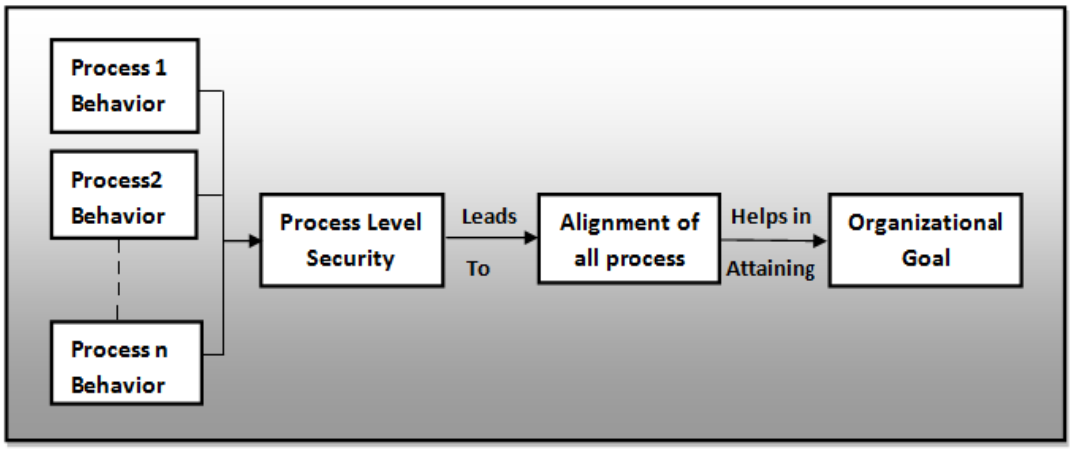

Figure 3. Interaction between Divisional level behavior and Business level behavior

Organizational Security

As discussed above, overall organizational level security requires various domains of security, like physical security, network security, etc., to be in position but organizational level security also requiresare working for.

This behavioral level security is most important because it cannot be even measured or audited and if not taken into consideration it can lead to undesirable behavior of employees' and thus chaos and non-fulfillment of the organizational goal. The Figure 4 represents the Information Security Behavioral Model, as follows:

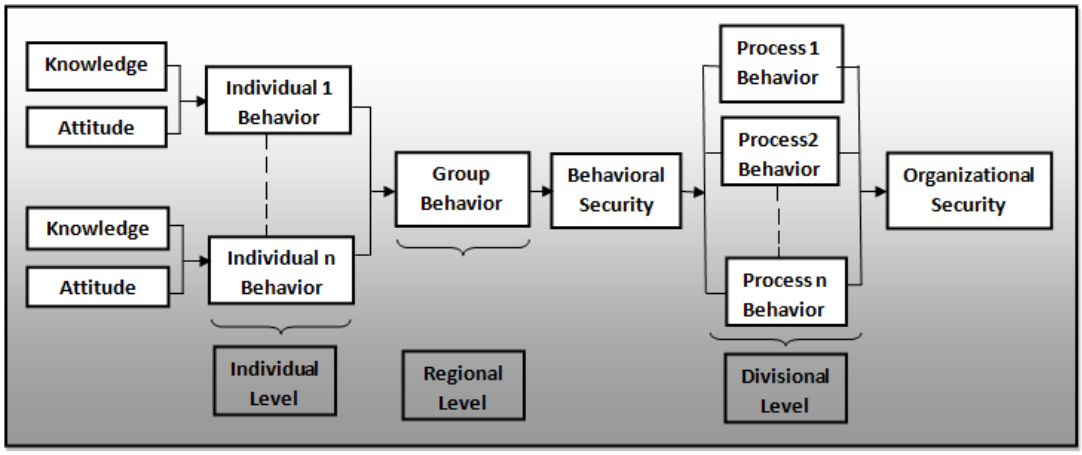

Figure 4. Information Security Behavioral Model

3. Methodology

To test the research model, a survey was conducted among 50 randomly selected employees' in an organization. The survey was questionnaire-based. This self-report survey question format has been an effective method for drawingand eliciting behavioral responses [12]. In the survey conducted for the study, three optional choices where provided: true, false, do not know. The survey questions included content relating to common information security issues and their solutions, such as viruses and anti-virus protection, firewall, web security, password security [8]. For each of the two constructs five questions were grouped which are the input to an individual's behavior in an organization: knowledge (affecting discretionary behavior) and attitude (behavioral component).

Voluntary participation of the employees' was taken and out of the total 60 distributed survey questionnaire 55 responses were received. From this data received 5 responses were deleted for missing data. A final of 50 responses were received. [8]

4. Findings and Discussion

In this paper SPSS version 16.0 for windows was used for statistical analysis of the initial inputs to an individual's behavior i.e. knowledge and attitude. For analysis of internal consistency reliability, the Cronbach's Alpha coefficient measurement method has been used. For this coefficient values over 0.9 indicate excellent internal consistency reliability, Figure 5 [8].

Cronbach's Alpha	N of items
.9	3

Figure 5. Realiability Statistics

The Cronbach's Alpha value for the two construct items in this study are 0.9. Therefore, the measures used in this study are considered to have excellent internal consistency reliability.

Further the Pearson correlation results shown in Figure 6 also support the research model discussed above. As shown in the resultant correlations matrix in Figure 6 an employees' attitude and knowledge towards using information security solutions both combines to give a behavioral security aspect. When the attitude is negative, for example, if there is conflict between individuals' values and company's values tension can arise. It's very often that people will not bear the tension for long time, and they will either change or modify principles or they may even leave the company [2]. Thus the impact will be on the processes they are involved in and ultimately the resulting behavioral security will affect the organizational goal. Similarly if the

knowledge has a negative impact, for example, due to inconsistencies between formal statements that are made my senior management and what actually a person experiences in practice around them, people will be guided more by what they see than by what they are told [2], then in such a case there will be lot of irregularities and will affect the behavioral security aspect of the individual as well as the process security will be affected and thus will have a negative impact on achieving the organizational goal.Thus the result indicates that the values for attitude and knowledge are related to behavior.

Correlations

		KNOWLEGDE	ATTITUDE	BEHAVIOUR
KNOWLEGDE	Pearson Correlation	1	.035	1.000**
	Sig. (2-tailed)		.811	.000
	N	50	50	50
ATTITUDE	Pearson Correlation	.035	1	.035
	Sig. (2-tailed)	.811		.811
	N	50	50	50
BEHAVIOUR	Pearson Correlation	1.000**	.035	1
	Sig. (2-tailed)	.000	.811	
	N	50	50	50

**. Correlation is significant at the 0.01 level (2-tailed).

Figure 6. Pearson Correlation

The positive correlations are quite strong as shown in the coefficient values. Thus, the result has validated the research model for information security behavioral aspects proposed in this study [8].

5. Conclusion

This study focuses on the relationship between an individual employee's knowledge and attitude in the domain of information security to give rise to his behavior towards the organization and thus providing a link on how such behavioral security aspect of every individual in an organization affects the alignment of various processes at the departmental level and thus affects overall business level goal of the organization.

From the findings it is validated that the attitude and knowledge reflects an individual's behavior towards adopting and using information security solutions and should be considered as an initial step before going for actual auditing.

References

[1] Sekaran U. Organizational behavior: text and cases. Southern Illinois: *Tata Mcgraw Hill Publishing Company Limited*. 2004.
[2] Leach J. "Improving User Security Behavior". *Computers and Security*. 2003.
[3] Vroom C, von Solms R. "Towards information security behavioral compliance". *Computersand Security*. 2004; 23: 191-198.
[4] "Information Security: End user behavior and corporate culture".*Seventh International Conference on Computer and Information Technology*. 2007.
[5] Pahnila S, Siponen M and Mahmmod A. "*Employees' behavior towards IS security policycompliance*". Proceeding of the 40th Hawaii International Conference on System Sciences (HICSS). 2007.
[6] Kruger HA, Kearney WD. "A prototype for assessing information security awareness". *Computers and Security*. 2006: 289-296.

[7] Lebek B, Uffen J, Breitner MH, Neumann M, and Hohler B. "*Employees' information security awareness and behavioral: A Literature Review*". Proceeding of the 46th Hawaii International Conference on System Sciences (HICSS). 2013; 12: 1530-1605.
[8] Wang PA. "Information Security Knowledge and Behavior: An Adapted Model of Technology *Acceptance". 2nd International Conference Education Technology and Computer (ICETC)*. 2010; 2: 364-367.
[9] Albrechtsen E. "A qualitative study of user's view on information security". *Computers and Security*. 2007; 26: 276-289.
[10] Albrechtsen E, Hovden J. "The Information Security digital divide between information security managers and users". *Computers and Security*. 2009; 28: 476-490.
[11] Stanton J, Stam K, Mastrangelo P, and Jolton J. "Analysis of end user security behaviors". *Computers and Security*. 2005; 24: 124-133.
[12] Grenier S, Barrette A and Ladouceur R. "Intolerance of uncertainty and intolerance of ambiguity: Similarities and differences". *Personality and Individual Differences*. 2005; 39: 593-600.
[13] Triandis HC. "Values, Attitudes, and Interpersonal Behavior". *Nebraska Symposium on Motivation 1979, University of Nebraska Press, Lincoln*. 1980: 195-259.
[14] Stanton J, Stam K, Mastrangelo P and Jolton J. "Analysis of end user security behaviors". *Computers and Security*. 2005; 24: 124-133.
[15] Abraham S. "*Information Security Behavior: Factors and Research Directions*". Proceeding of the Ameican Conference on Information Systems (AMCIS). 2011: 462.
[16] Pahnila S, Siponen M and Mahmmod A. "*A New Model for Understanding Users' IS Security Compliance*". Proceeding of the Pacific Asia Conference on Information Systems (PACIS). 2006.
[17] Albrechtsen E. "A qualitative study of users' view on information security". *Computer and Security*. 2006: 276-289.
[18] Albrechtsen E, Hovden J. "The information security digital divide between information security managers and users". *Computer and Security*. 2009: 476-490.
[19] Labek B, Uffen J, Breitner MH, Neumann M, Hohler B. "Employees' Information Security Awareness and Behavior: A literature Review". *46th Hawaii International Conference on System Sciences (HICSS)*. 2013: 2978-2987.
[20] Spurling P. Promoting security awareness and commitment. *Information Management and Computer Security*. 1995; 3(2): 20–6.
[21] Stanton JM, Stam KR, Mastrangelo P, Jolton J. Analysis of end user security behaviours. *Computers and Security*. 2005; 24(2): 124–33.
[22] ISF. "The standard of good practice for information security". Version 4.0. *Information Security Forum*. 2003.