INFORMATION SECURITY CULTURE SUBJECT DOMAIN

Aleksandr POTII[1], Dmitry PILIPENKO[2], Inna REBRIY[1]

[1]Kozhedub Air Force University, Kharkiv; [2]Kharkiv national University of Radioelectronics

e-mail: potav@ua.fm, frtwork@gmail.com

Abstract

Today we can say with certainty that organizational aspects of Information Security should be managed, controlled and evaluated equally with technical aspects. Evaluation of human activities in terms of Information Security can be studied within the concept of "Information Security Culture", which has been widely used by scientists during the last decade. Complex nature of this phenomenon forced researches to use a wide range of models, approaches and concepts for deeper understanding. Thus too wide and separated subject domain was created, which considerably complicates further research. This article addresses this problem by means of developing ontology models of Information Security Culture and Information Security Institute subject domain.

***Keywords**: information security culture, information security institute, security center, security agent.*

1 INTRODUCTION

Understanding the problems of Information Security (IS) assessment and management undergoes qualitative changes. The scientists and experts in the field of IS express the idea that organizational aspects of IS are at least as important as technical ones [1, 2]. It should be noted that organizational aspects of IS are often underrated due to their qualitative nature and the difficulty of assessment.

This leads to the following problem: the human factor and information security culture (ISC) particularly should be studied based on system approach. As security incident reports show, the great deal of security incidents happen due to policy violation by organization's own members [3].

This paper considers the aspects of information security institute (ISI) development, connection between the main components of ISC and the key problems of ISC promotion.

2 INFORMATION SECURITY INSTITUTE

Modern organizations still suffer from accidental security incidents happened on the account of their own personnel, despite of adequate security policies (measures, procedures, practices, controls, etc). The major part of the employees treats IS policies as obstacles and limitation. Such poor understanding of the goal and the purpose of IS policies leads to security policies violation. The issue of IS policies non-compliance has two major solutions:

1. The implementation of a strict inspection system with administrative penalties and fines for information security violation. This solution is capable of producing quick result, though its negative perception by employees makes the effect nondurable. Apart from this shortcoming, continuous supervision leads to the growth of expenditures inevitably, which can be unsuitable for small business or small organizations.

2. The other solution is to promote and maintain a high level of ISC. Though this is rather a long-term result-oriented option, it promises a long-lasting effect in case of success. The promotion of ISC leads to reduction of security risks connected with the organizational aspect of information security. While ISC is maintained at the high level, security functions would not be weakened, oversimplified or minimized over time.

ISC should be considered as part of more complex structure – information security institute (Figure 1). The main function of ISI as a social institution is to coordinate the employees' professional duties and the business activities of the organization in terms of IS. Figure 1 shows the connections between the main components, which form the core terminology of the subject domain.

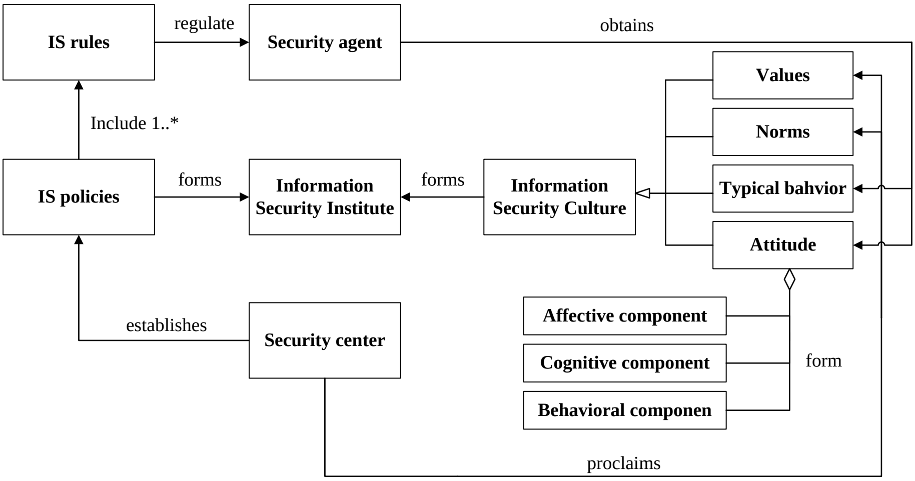

Figure 1 Ontology model of ISI and ISC subject domain

The following definition of ISI is proposed: *Information Security Institute* is an ordered and formalized system of shared values, standards of behavior, security regulations and principles, which are used to coordinate the main business goals with security agent's activities in the context of information security.

The development of ISI is influenced by two subjects, namely: security center and security agent. Security center can be represented by the top management, Chief Information Security Officer or other agent of management, whose interests should be secured. Security agent is usually represented by an average executive or other person, who takes no part in the decision making process directly.

Security center is an agent of management, who performs a set of control actions with ultimate goal of establishing information security institute.

Security agent is a person, whose actions and behavior influence the promotion of information security culture through information policy compliance.

ISC and security policies should be considered as instruments for information security activity management in terms of institutional management. The nature of institutional management can be described as follows: creation and managing of limitations, norms and rules in the context of IS. Traditionally norms and limitations can be expressed in explicit or implicit form. ISC thus should be put to implicit form of norms and limitations, while security culture should be put to the explicit one. The essential moment of institutional management is that IS policies perform the regulating role ad ISC performs the motivating role.

3 ISC SUBJECT DOMAIN

The analysis of publications shows that researchers are considering the human factor as the main cause for security incidents of organizational nature. It also indicates that ISC is a complex concept, which should be considered as a certain security component of organizational character. System approach should be used in order to perform a more detailed research.

3.1 The definition of Information Security Culture

It should be noted, that there exists no uniform system of notions and terms. Researchers use different models and approaches in order to investigate the concept of ISC, which creates too wide subject domain. Many definitions of ISC exist, which emphasize different aspects of ISC. As stated in [4], ISC is investigated in terms of different approaches and concepts: awareness maturity, Detert's framework, E. Shein's model of organizational culture, shared values, organizational behavior, human resource management for education and learning, socio-technical perspective, Hall's taxonomy. Still, these definitions have some common points, which allow us to generalize definition of ISC: *Information security culture* is a set of values, norms and standards of behavior, which forms acceptable behavior in terms of information security.

ISC may cause positive or negative effect on organization’s functioning, depending on its high or low level. For example, non-compliance to IS policies is often typical for many organizations. According to the survey presented in [5], most of employees are confident that responsibility for integrity of information assets rests solely on security staff, and their task mostly consists of eliminating mistakes and IS incidents aftereffects. One of the respondent organizations had an awareness campaign conducted by security department (on their own initiative) via corporate e-mail. The main goal of this delivery was to make employees aware of IS functions and to inform them about changes in information security policies. The initiative was unsuccessful, since the majority of employees deleted these messages without reading them. Thus values, norms, standards of behavior and attitude towards IS requirements should be fostered deliberately, since otherwise they will be formed spontaneously.

3.2 The main components of ISC

The concept of values. Values should be interpreted as the most important person’s objects and phenomena, which present his goals and guidelines of his life [6]. Values can cause either positive or negative effect on organization’s functioning. When speaking of values, we mainly refer to positive values, which support organization’s strategic goals and mission.

Values can be formed either spontaneously or intentionally – by the agent of management. Spontaneously developed values are usually negative by its nature in the context of IS, since most of the people have no intention to comply with security requirements initially. IS policies are often interpreted as obstacles and limitations, thus such attitude should be changed. The most obvious way of changing such attitude is raising the competence and awareness of the employees. Understanding the role and purpose of IS policies is essential for compliance. The examples of positive values are: information assets safety, employee discipline, motivation, loyalty, initiative etc. The process of values acceptance by employees is greatly influenced by support of the management. In case when agent of management proclaims certain values, it serves as tacit signal for employees, which emphasizes the importance of IS policy compliance.

The concept of norm. Norms can be described as a set of requirements towards a person or group, who occupy a certain place in organizational structure [6]. While development and acceptance of norms progresses parallel with development of values, norms are still less stable than values. Norms are dynamic by nature and consist of motivating and mandatory components, thus norm can be affected by different factors. Virtually norms are followed, until they are functionally useful for organization, group or person. Otherwise norms can be formally recorded in some kind of normative document, but be ignored practically.

Norms, as well as values, can be formed either spontaneously or intentionally. Norms of behavior serve to regulate, guide and assess behavior of the employees. The employee’s typical behavior in the context of IS creates conventional norms of behavior, so established norms may not be necessarily positive and useful for organization.

As dynamic component norms of behavior can be developed or changed at different levels of the management. In case of spontaneous development (without proper control), there is a probability, that norms will change over time, not necessarily in positive way. This indicates the importance of management commitment principle in terms of organizational aspect of IS.

The concept of attitude. Positive attitude towards IS policies is one of conditions of successful ISC promotion. Attitude in terms of IS should be interpreted as an aptitude of person to behave in a certain manner under certain circumstances. Attitude should be considered as a three-component framework, consisting of affective, cognitive and behavioral components [7].

Affective component is usually referred to some phenomenon, event or particular person within the organization. That's the way of human nature to evaluate objects and phenomena around him and to create a perceptive image. This image contributes to the development of ISC and consolidates an overall attitude as well. For example, recognition of supervisor's authority or subjective evaluation of the importance of sensitive information can be considered as an affective component. Employee prejudice will inevitably negatively influence an attitude.

Cognitive component represents the knowledge about certain object or phenomenon. The ultimate belief will greatly influence an attitude depending on the level of underlying knowledge. The cognitive component (unlike the affective component) has no emotional character. This means it's possible to change cognitive component via rational evidence. For example, basic IS training can lead to the growth of awareness and competence. Awareness and competence reduce the probability of IS incidents of organizational character, caused by lack of knowledge.

Behavioral component defines the aptitude of individual to act in a certain way. This component contributes the most, due to its nature and influence over the other components. For example, a negative experience of personal involvement in security incident due to IS policies violation affects the behavioral component. This also develops a new knowledge, which improves awareness and makes employee perform their routines in more secure manner.

Figure 2 illustrates connection between the components of attitude and IS policies. Awareness and competence (cognitive component) are necessary for security policy compliance, still they cannot guarantee the stability of such behavior. Apart from basic knowledge employee should possess intention (behavioral component) to comply with IS policies and perform his daily routine in secure manner [8].

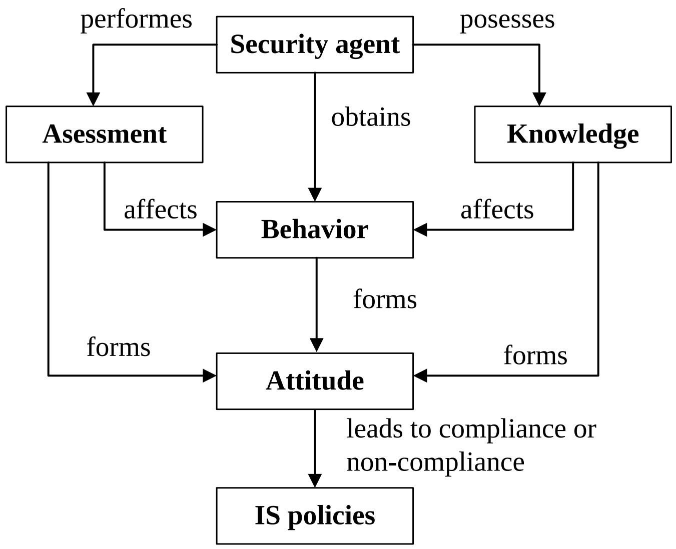

Figure 2 Relations between attitude components and IS policies

The value of data circulating within the organization is not equal for different persons or even departments. If we treat employees from the perspective of rational egoism, we can say that effort put to protection of information is equal to their subjective assessment of this information's value [9]. Thus both knowledge and correct behavioral choice equally affect the compliance of IS policies. From organizational perspective IS policies can be considered effective only in case they are practically followed.

This problem raises an obvious question: which factors influence the discussed components and the intention to comply with IS policies. Many researchers agree that adequate IS policy is not enough to guarantee the absence of security incidents, caused by employees. Survey conducted in a number of organizations revealed that utmost correspondence between the formal IS policy and day-to-day activities showed organizations with high level of ISC.

The concept of typical behavior. According to the theory of organizational behavior, each member of the organization beginning with regular employee and ending with top management possesses a set of needs, expectations and interests, viewpoints, attitudes and concerns [10]. All these aspects have influence over development of typical behavior. Drawing a line between acceptable and inadmissible behavior in terms of IS, ISC demarcates employee standards of behavior. Norms of behavior serve for control of deviant behavior and promotion of etalon standards of behavior. Typical behavior develops in accordance with norms and values, whether they are positive or negative. The other factor that influences typical behavior development is the knowledge of employee, since there is a straightforward relation between behavioral choice and knowledge (Figure 3).

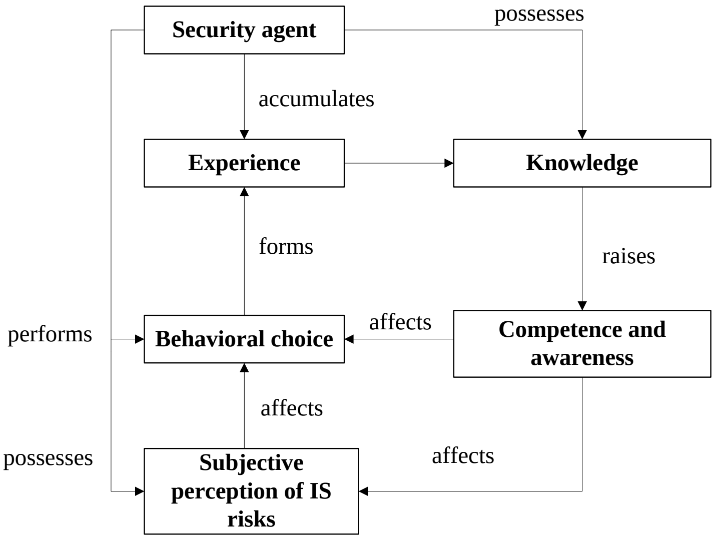

Figure 3 Relations between behavioral choice and knowledge

As shown in Figure 3, competent employee has basic understanding of threats, vulnerabilities and risks; understands possible consequences of security incidents for organization, colleagues and himself particularly. In the context of IS, such set of knowledge can be developed via learning or in practice, as a form of experience. A more sound understanding of IS functions and goals can positively affect behavioral component of employee. The growth of knowledge influences the subjective perception of risk.

While performing certain actions an employee acquires experience and consolidates ISC as well, since typical behavior transforms into standards of behavior over time. There are some other factors that affect behavioral choice, namely normative beliefs and established standards of behavior.

Normative beliefs are individual's perception about the importance of other people's judgments of his particular behavior. An *established standard of behavior* is represented by typical behavior of every member of the organization: regular employees, top management, security staff, etc. In other words, if there is a rule to performance daily activities in secure manner, it works as a signal, that indicates the necessity of IS policies compliance.

New employees find themselves in the phase of adaptation and are guided by established standards of behavior, gradually adopting the way the community behaves itself. Employees' activity is thus regulated through acceptance of organizational culture.

However a certain paradox should be mentioned: while regulating activities, ISC is a product of personnel activity. Employees develop an idea of acceptable behavior during the process of socialization. This process helps an employee to adopt the established values, norms, patterns of behavior (regardless of its positive or negative character). The process of socialization becomes a useful tool of shaping employee behavior in case of top management support (Figure 4).

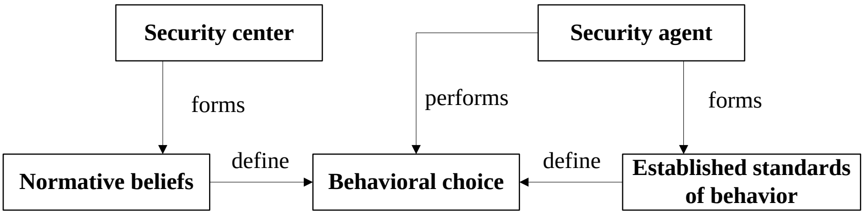

Figure 4 Relations between the established standards of behavior, normative beliefs and behavioral choice

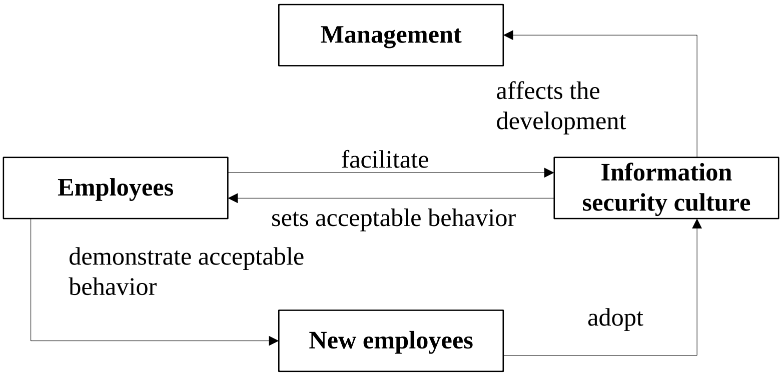

Figure 5 The process if socialization

4 CONCLUSION

The management and control of organizational aspects of IS should be performed in terms of institutional theory. In the context of IS this implies establishment of ISI as a two-component structure. On the one hand, ISI is based on IS policies and reflects the administrative component of IS, which is implemented by enforcement mechanisms. On the other hand, ISI includes ISC – a motivating mechanism, which is aimed at security policies compliance. Seeking balance between these mechanisms is the main difficulty of managing organizational aspects of IS.

ISC should be regarded as an important component of information security system and should not be formed spontaneously. ISC should become an object of great attention in management perspective, since its development and maintenance significantly depends on management commitment.

The main actors of security (security center and security agent) are active components of information security system. Whether IS policies are complied depends on many factors: the level of competence and awareness, basic knowledge, shared values, attitudes and behavior of security agent.

The further research should be focused on development of method for ISC assessment and more detailed research of discussed ISC elements and relations between them.

REFERENCES

[1] DHILLON G., TORKZADEH G. Value-focused assessment of information system security in organizations. Proceedings of the International Conference on Information Systems, ICIS 2001, December 16-19, 2001, New Orleans, Louisiana, USA.

[2] SIPONEN M., OINAS-KUKKONEN H. A review of information security issues and respective research contributions. Volume 38 (1), February 2007, P. 60 – 80.

[3] InfoWatch Global Data Leakage Report: http://infowatch.com/

[4] LIM J.S., CHANG S., MAYNARD S., AHMAD A. Exploring the Relationship between Organizational Culture and Information Security Culture. 7th Australian Information Security Management Conference – Australia: Edith Cowan University, 2009. – P. 88 – 97.

[5] ALFAWAZ S. Information security management: a case study of an information security culture. PhD thesis, Queensland University of Technology, 2011. – 301 p.

[6] STEKLOVA O.E. Organization culture. – Ulyanovsk: UlSTU, 2007. – 127 p.

[7] SCHEIN, E. H. Organizational Culture and Leadership – Jossey Bass, 3rd Edition, 2004. – 464 p.

[8] NIEKERK J.F. Fostering Information Security Culture through Integrating Theory and Technology. Ph. D. thesis – Nelson Mandela Metropolitan University, 2010. – 302 p.

[9] BIRI K., TRENTA G. M. Corporate Information Security governance in Swiss Private Banking. Master’s Thesis. – Executive MBA Program of the University of Zurich, July 2004. – 79 p.

[10] MYERS D. Social psychology. – S.-Peterburg.: Piter, 1997. – 688 p.