**[TITLE]Information And Knowledge Management in The Scope of the Information Security Practices**

[Name] Mohd Sharulnizam Bin Kamarulzaman

Faculty of Information Management,

[Affiliation] UiTM Selangor Branch, Puncak Perdana Campus, 40150 Shah Alam, Selangor, Malaysia

Received Date: xxxx

Publish Date: xxxxx

**Abstract.** Information security has always been an important requirement for the business. Such assets can be broken down into three main areas, namely people, process and technologies. The Internet, the proliferation of the web, networks and the ever-growing presence of innovation has triggered profound changes to procedures that are integral in individual and institutional routines. Such technological changes have led to an increase of competitiveness which decentralization and have contributed to the need for leadership, command, security, information and knowledge safety. The article presents the findings of an information security investigation, which examines the involvement with human aspects in the field of information security and knowledge management. The implication is that the "people" component is an important variable, even crucial, for the management of information security in organizations. It can be concluded that the human element is an important, perhaps critical, parameter for the management of corporate information security.

**Keywords**: information security, information and knowledge management, informational behavior

1. [HEADING] Introduction

Business demands meet the need to find strategic business solutions (Hussin, Hashim & Yu, 2018). In the business world, the concept of what is security has been evolving and is no longer restricted to the technical issue. From this perspective, information security emerges as a relevant resource, since it seeks to link to the company's business variables that influence the protection of informational assets. These variables are now seen as integrating elements of the core business, as safeguarding information and knowledge is critical to success, competitiveness and survival in the globalized market.

We advocate here the need to integrate, in an integrative way, the elements "people", "processes" and "technologies" as variables that coexist in companies and that need to be treated with balance and equal conditions in the context of security management of the company’s information (Sveen, Torres And Sariegi, 2009).

The change to this analysis bias implies abandoning the exclusive dependence on technological aspects and turning attention to the subjectivity inherent to human beings, their relationships and their behaviour in organizations since such behaviour greatly influences information security management. Colwill (2010) points out that, even considering other equally relevant factors, overconfidence in technology will lead to unexpected results in handling a very critical internal security threat: the human element. This element poses information security risks, as people can gain legitimate access to information, know the organization, and know where valuable assets are located.

This article focused on the identification of human aspects interference in information and knowledge management practices concerning information security. These aspects are, in fact, inherent in the human condition: people's behaviour, relationships, and conduct affect the business environment at a spectrum of varying levels where information security is needed.

Companies organize themselves in global markets to maintain competitiveness and their standard of work. Technology is the catalyst that supplies companies with efficiency and effectiveness. However, sophisticated as a technology solution may be, it will be just another element of the process of maintaining the organization's competitiveness. People and processes are critical elements and only strategic management that consider all components of the organization - planning, effective action and strategic handling of information - can achieve the levels of competitiveness that the company needs.

Thus, by reflecting on how human resources interfere with an organization's information security, it is easy to see that the “people” element is vulnerable. This vulnerability manifests itself through two inter-dimensions, both of which interfere with information security and make the human factor the weakest link: First, employees should ideally have sufficient information security knowledge to effectively implementation and maintenance of security controls, which does not always occur; Second, employees must have the right attitude toward information security, but sometimes they have not been told how to do that (Niekerk and Solms, 2010).

This first approach brings reflection on the need for transparency, management and effective communication regarding the information security guidelines adopted by a company. All elements of the organization must be synergistically involved so that they can deal with security issues, developing completeness of actions and real awareness of the need to safeguard organizational assets. Kraemer, Carayon and Clem (2009) contribute to this perspective by noting that users are not necessarily anti-security, but often unable to determine the security implications of their actions.

This scenario leads to the reflection on how the lack of knowledge generates inappropriate behaviour because of the expected information security actions since acting correctly develops entirely from the prerogative of knowing how to act. It is, therefore, crucial for organizations to pay attention to maintaining and sharing reliable information for corporate information and knowledge management, as well as for a better understanding of their users' needs. Information users should be perceived as those who are not only driven to seek information for cognitive purposes but as beings who live and work in social environments (such as companies) and who, in their context, create their own motivations for learning, seek information and satisfy their needs (Wilson, 2006b). This information user is defined in this article as one who is strongly dependent on information and uses it for specific purposes, such as professional purposes.

1. [HEADING] Literature Review

*[Sub-Heading]*

In reflecting on how people might adopt safe behaviour, it is noted that clarification is needed on what is safe behaviour and its relationship to information security and its elements such as risk minimization, protection of information assets, and, positioning to preserve itself from attacks. From Jean Piaget's work, that knowledge has a specific goal or purpose of helping the person to adapt to the environment. This scenario demonstrates that in the corporate environment, employees intentionally or negligently employed, and often due to lack of knowledge, are the biggest threat to information security. Making people aware of the importance of an appropriate level of user cooperation and commitment to knowledge building is paramount, given that without such contributions, security techniques can be misused or misinterpreted by users, thus ineffective. That is why information security depends on both knowledge and human cooperation. The expectation is that lack of knowledge can, in most cases be addressed through education; Lack of cooperation can be addressed by promoting an information security sub-culture in the organization (Niekerk; Solms, 2010).

It is understandable that these approaches lead to reflection on how factors related to knowledge production and people's cooperation are critical elements of the human variable in information security management. Similarly, elements such as knowledge sharing, organizational learning and intellectual capital management bring tone to the proposed approach and provide a breadth of vision and development of comprehensive organizational actions to manage human resources. However, we realize how much people need to be seen as potential risk promoters in the corporate environment because through this perception, more quickly, the security breaches generated by these people can be understood and the appropriate actions implemented.

This view once again confirms the importance of promoting the development of knowledge, cooperation and organizational learning among employees aiming at the dissemination of information on information security. This dissemination of information enables instruction to be considered before the need for a corrective attitude. It is also emphasized that risk assessment models can assist in the task of promoting knowledge production since they can be seen as auxiliary learning mechanisms in the organizational learning process. Making a correlation between risk assessment and organizational learning, it is noteworthy that if the perception of security through risk assessment increases, the company learns more and, consequently, the learning rate and the body of information security knowledge increase, reinforcing the company's ability to detect security breaches and employees to act more consciously (Sveen; Torres; Sariegi, 2009). In short, it can be said that safe behaviour is something to build and should be among the goals of organizations. The process of acquiring knowledge and building meaning is essential for people to have safe behaviour, since, as already mentioned, acting develops exclusively from the prerogative of knowing how to act. It is possible to intervene in such a way that a person has a safe behaviour as soon as that person understands what it means to have a safe behaviour and can proactively act in response to the stimuli from the environment.

It is assumed that the threat to insider information and information security cannot be eliminated entirely but can be controlled, evaluated and managed. By understanding the human factors linked to information security, it is possible to gain a better understanding of the real risks that organizations face in today's global business environment. Information and knowledge management must be effective in this regard. Informational use must be controlled so that any abnormal behaviour is investigated and containment actions are quickly implemented.

1. [HEADING] Conclusions

The information security perspective developed in this article reported issues involving corporate information sources, the needs of information users for corporate users, and the corporate guidelines that permeate the entire life of the organization. The variables involved in creating a safe behaviour for the information user as well as information security from the point of view of human resource management were briefly described. Thus, it was concluded that the importance of education and organizational learning in information security issues is fundamental. While many information security initiatives are driven by information technology departments, the real reasons for the failures continue to pervade the entire organization. People are present everywhere, whether as users or as developers of information systems, and it is up to them to watch out for organizational policies and guidelines designed to maintain security. It is up to the organization and its management body to make such policies and guidelines known and to value their adoption.

Such dissemination occurs within and outside the organization, as other business partner companies and their employees have access to confidential information from third parties. It was concluded that the “people” element is a critical variable in information security management in organizations. Information policies should be accessible to employees and enforceable. Regarding technology, investment continuity is valid, but it must be balanced with the development of informal controls (involving people) and formal controls (involving policies and processes) for effective and effective information security management.

References

Allen, B. L. *Toward a user-centered approach to information systems*. Los Angeles: Academic

Press, 1996.

Beautement, A., & Sasse, A. (2009). The economics of user effort in information security.

*Computer Fraud and Security*. https://doi.org/10.1016/S1361-3723(09)70127-7

Colwill, C. (2009). Human factors in information security: The insider threat - Who can you

trust these days? *Information Security Technical Report*.

<https://doi.org/10.1016/j.istr.2010.04.004>

Cyber Security Malaysia, MS ISO/IEC 27001:2007 Information Security Management System

(ISMS) Implementation, ed. Malaysia: Cyber Security Malaysia, 2010.

Da Veiga, A., & Martins, N. (2015). Information security culture and information protection

culture: A validated assessment instrument. *Computer Law and Security Review*.

<https://doi.org/10.1016/j.clsr.2015.01.005>

Everett, C. (2008). The right medicine. *Infosecurity*.

[https://doi.org/10.1016/S1754](https://doi.org/10.1016/S17544548%2808%2970149-9)

[4548(08)70149-9](https://doi.org/10.1016/S17544548%2808%2970149-9)

Haris@Harib, A. R., Sarijan, S., & Hussin, N. (2017). Information Security Challenges: A

Malaysian Context. *International Journal of Academic Research in Business and Social*

Sciences. <https://doi.org/10.6007/ijarbss/v7-i9/3335>

Hussin, N., Hashim, H., & Yu, H. (2018). Strategic Information Management (SIM) In Mala

sian Organizations: An Investigation of its Antecedent. International Journal of Academic

Research in Progressive Education and Development, 7(3), 291–304.

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer

and information security: Pathways to vulnerabilities. *Computers and Security*.

<https://doi.org/10.1016/j.cose.2009.04.006>

Marchionini, G. Digital Library Research and Development. *Encyclopedia of Library and*

*Information Science*, v.63, p.611-19, 1998.

Norhayati Hussin & Adnan Jamaludin (2018). Information Behavior of Managers (IBM) and

Strategic Information Use (SIU) in Malaysian Industries. International Journal of Engineering

& Technology, vol.7 , p. 249-252.

Sveen, F. O., Torres, J. M., & Sarriegi, J. M. (2009). Blind information security strategy.

*International Journal of Critical Infrastructure Protection*.

https://doi.org/10.1016/j.ijcip.2009.07.003

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext

social engineering threats to information security. *Journal of the American Society for*

*Information Science and Technology*. https://doi.org/10.1002/asi.20779

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management

perspective. Computers and Security. <https://doi.org/10.1016/j.cose.2009.10.005>

Wilson, T.D. Revisiting user studies and information needs. *Journal of Documentation*, v.62,

p.680-684, 2006b.