INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 10, Issue 11, (2020) E-ISSN: 2222-6990

Information and Knowledge Management in the Scope of the Information Security Practices: The Human Factor within Organizations

Mohd Sharulnizam Kamarulzaman, Norhayati Hussin, Mohd Shamsul Mohd Shoid, Azmi Ab Rahman, Mohd Nazir Ahmad, Rafidah Abdul Aziz

Faculty of Information Management, Universiti Teknologi MARA (UiTM) Selangor, Malaysia

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v10-i11/8185 DOI:10.6007/IJARBSS/v10-i11/8185

Published Date: 28 November 2020

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 have 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 crucial, parameter for the management of corporate information security.

Keyword: Information and Knowledge Management, Information Security, Informational Behavior, Information Security Investigation, Knowledge Safety

Introduction

Business demands meet the need to find strategic business solutions. 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. Fenz et al (2014) state the information security is

important to organization however it is challenges to prove factor contribute on it. These challenges and situation occur because the easiness access the digital data and information which deployed by the organization (Harib, Sarijan & Hussin, 2017).

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 people, process and technologies relies in each another for successful implementation of security management in the organization. According to Tarun (2018), the singel and integrated framework which overlapping with the strategy based on security tools, people and process will yield the effective defenses.

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.

Information and People Security: A User-Centered Management Approach

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 effective 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 respond. It is therefore, crucial for organizations to pay attention to maintaining and sharing reliable information for the purposes of 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.
This process of seeking information, according to Marchionini (1998), is driven by the informational need of the individual. The extreme variety of informational needs of individuals makes the task of enumerating them complex and difficult (Allen, 1996). Marchionini (1998) and Allen (1996), highlights that in the search and use of information process, its value resides in the relationship that the user builds with certain information. Thus, several elements affect information search patterns and information behaviour as a whole, such as the variety of information sources, different types of users, user needs and preferences, among others.

From this perspective, the choice of information sources by a given user is oriented according to their preferences, needs, accessibility, environment, etc. This is because information is valuable resources required, therefore acquired and using information is critical and important activities (Kadir et al, 2018). It also suggests that information sources are classified into the following categories: internal and personal, internal and impersonal, external and personal, and external and impersonal. It is observed that in this process of need and informational search, the resource made available through electronic information, structured in various ways, has become a dominant environment. The engagement between the relationship of the information seeker with the world wide web, with digital libraries and with other information structures is becoming stronger (Wilson, 2006c).

For this reason, the understanding of users' informational needs goes through the information search behaviour and results in recognition of some perceived user need.
This behaviour can be determined in many ways, either through user demands on formal systems (information systems), claims about systems that can perform information functions aggregated to a primary or non-primary function, and finally by seeking information through someone else, through information exchange (Wilson, 2006b). Beyond the informational search, it is the behaviour that highlights the information needs the only basis on which to judge the nature of the informational need and its satisfaction. Putting these perspectives together, it can be concluded that information needs are explanatory constructs that help to understand informational behaviour (Allen, 1996). This thinking

makes us realize that in order to build information security behaviour in an organization, it will be necessary to interact with elements pertinent to Information Science and that these elements feed a trajectory that begins with the need for information goes through the informational search and ends with informational behaviour. In fact, the behaviour of need, search, and informational use is a process of meaning construction. This meaning construction occurs when the user creates meaning from the information found, moving from a state of uncertainty and uncertainty to clarity and confidence.

Building Safe Behaviour

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 it is 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 collaboration can be addressed by promoting an information security sub-culture in the organization (Niekerk; Solms, 2010).

Understandably, 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 the 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.

Objectives and strategic planning will include actions at the operational, tactical and strategic levels of the organizational structure. Much has been discussed about the correlation between disgruntled employees and internal attacks that result in security threats. This issue deserves special attention since it can only stereotype people by misleading judgments about the elements involved, such as union leaders and employees with real complaints. A true motivation analysis for betrayal requires complex psychological lifting and varies from individual to individual. Shaw et al. (1999) apud Colwill (2010) identify six personal characteristics that have direct implications for risks of a potential malicious intruder:

- The false sense of lack of recognition and right, resulting in a desire for revenge;
- Anger and social frustrations, alienation, resistance to authority;
- Computer dependence and aggressive loneliness, desire to explore networks, break security codes, and challenge security professional's safety;
- Ethics and flexibility without moral inhibitions that prevent malicious behaviour;
- Loyalty reduction, when the element identifies more with its computer profession or speciality than with your employer;
- Lack of empathy and neglect or inability to appreciate the impact of the behavior of others.

Colwill (2010), still in his interpretation of NIAC (2008), concludes that people who commit malicious actions are from the privileges that they have and from the experience of causality or mechanism that affects motivation that leads to betrayal. These experiences can be classified into three primary sources: growing discontent; hiring by hostile outside entities or groups, and the infiltration of the malicious actor into a position of trust. When these elements are crossed with the imperative of developing cooperation and shared knowledge in companies, while considering variables intrinsic to the human personality - opportunity, motivation, ability and discontent - it is observed that more than ever organizations need strategies to deal with human resources (Beautement; Sasse, 2009).

People can develop feelings from experiences and act in ways that undermine the organization. This is why it is very important for organizations to act proactively in developing and encouraging cooperative actions among employees and also between the organization and its employees. Nevertheless, there is a need to promote actions that will contribute to the expansion and sharing of knowledge in companies in order to create awareness in people and bring them closer to the organization.

It is worth highlighting the perspective of trusted employees who also support each other: they trust and expect, in return, even to receive trust, and that is why organizations must be careful to provide this balance. By acting in this way everyone benefits, since on the part of employees, there will be a commitment to the protection of sensitive information of the organization; and on the part of the organization, there will be efforts to provide some kind of protection (Workmann, 2007).

The synergy between organization and employees is paramount in maintaining an organizational culture that focuses on the security of information assets. At the same time, the development of cooperative actions, knowledge dissemination and organizational learning is facilitated by the synergy between the parties. The proper connection between

employers and employees is so important that it is generally noted that organizations cannot protect the integrity, confidentiality and availability of information allocated in a networked environment without ensuring that each person involved understands their roles and responsibilities, as well as being trained to carry them out.

Thus, a user must be aware of specific operational controls, as the efficiency of the process depends on their behaviour. To ensure this required level of knowledge, ostensive training, awareness and educational programs will be required (Niekerk; Solms, 2010). From the perception that information security is not just a technology issue, it can be seen that organizations agree on the need for employee behaviour change to achieve higher levels of protection in accordance with your security policies. However, the path taken to achieve this goal is often wrong, as most of the time companies only adopt a threatening attitude towards workers imposing sanctions if policies are not followed (Beautement; Sasse, 2009).

The perspective approached so far leads to believe that efficiency in human resources management, from the perspective of corporate information security needs, is linked to the relationship that the organization establishes with its employee. In this sense, all efforts to make this employee aware, develop a culture of knowledge sharing, collaboration and organizational learning will not work if the company adopts a threatening attitude towards employees and is guided by the promotion of employee coercion.

It is noteworthy that an attitude of fear, coercion and threat is quite different from the adoption of management methods as in the case of sanctions and rewards. Therefore, a change of beliefs and values comes from the results of learning processes based on successful behaviour. Thus, comments, rewards and sanctions are management mechanisms that should be used correctly to ensure that employees understand what would be considered successful behaviour (Niekerk; Solms, 2010).

In line with the need to change employee behaviour, education appears as an option and is often the only way to convince employees and managers about the need to do things differently. For a paradigmatic change in the organization, it is vital to teaching employees what to do, how to do it, why it should be done in a certain way, or why this or that conduct should be adopted (Niekerk; Solms, 2010). If the employee has been given the knowledge and education, they will make sure their work and organization safe (Aronovish, 2018).

Everett (2008) contributes by suggesting that employee training and education are key factors in gaining or raising awareness about the value of data manipulated within the organization and, respectively, the role of each individual in the organization to safeguard this asset. Therefore, awareness must be an intrinsic component of organizational culture and must be measured before and after any change promoted. The tools used for such measurement are surveys whose results can prove understanding of the proposed change and, more directly, through requests for password renewal and reduction of incidents of improper or unauthorized access to the company. Information Security Management System (ISMS) provides guidelines for employee education, specifying that it should include security requirements, legal responsibilities and corporate controls, as well as training in the proper use of information processing facilities before access to information or services, is granted. This guideline refers to various relevant standards, such as ISO/IEC 27001:2005 ISMS (CyberSecurity Malaysia, 2010).

However, the difficulty of building strong informal controls has led to a kind of compensation that has been achieved through the construction of very strong formal controls (policies, standards, guidelines, etc.). This can be seen from the large number of information security standards such as ISO 1799 and COBIT. However, there is no way to guarantee the fullness

of formal controls without the parallel development of informal controls. The particular characteristics of the culture of each company impose adjustments to the set of safety standards when implementing them.

For this reason, there is a difference between what is written in the standards and what is actually practised in companies (Sveen; Torres; Sariegi, 2009). The goal of fostering information security behaviours makes people supportive of protecting information assets in accordance with the organization's policies regarding information security and based on the code of ethics. The success of security behaviours would lead to higher rates of security incident reporting, adherence to a clean table policy or deletion of confidential documents (Harib, Sarijan & Hussin, 2017; Alevriadou & Massi, 2013), which investigates how information security is perceived, suggests that such perception is the mechanism by which a person assesses information security threats, which in turn determines his behavioural response. On the other hand, it is identified that a high workload can create a conflict of interest between functionality and information security. In addition, high workloads are associated with a human error during system use (Kraemer; Carayon; Clem, 2009). Protecting organization information is the responsibility of all employees. Education, training and awareness-raising are the most efficient non-technical measures available from the perspective of the human element and information security. Safety requirements should be integrated into people's behaviour as a normal activity through clear policies and education. Many problems of leaking confidential information come from ignorance rather than malicious intent. In addition, accidental failures can have major impacts.

It is observed that in many companies, the issue of security and education are mandatory requirements, audited from the legal perspective. A focus on the change needed is to measure workforce behaviour as part of the organizational development plan. Basic training and instruction can be adopted, but the emphasis should be on security integration and awareness, as well as understanding the organizational culture. Employees must change their behaviour to protect their assets and information. To achieve this goal, in addition to raising employee awareness, it is necessary to incorporate security needs into the organization's cultural values. For real safety effectiveness, one should go beyond just following security policies, but working on a process of building empathy, understanding, ownership, and developing knowledge about situations that can cause safety risks, behaviours, and reactions (Colwill, 2010).

Thus, the way in which the information is processed by the individual, in the group and consequently in the company culture is a critical evaluation factor for solidification of values and in parallel with the creation of striking impressions in the employees. The culture of information security, that is, perceptions, attitudes, and assumptions that are accepted and encouraged in an organization, as well as the way things are done in an organization to protect information assets, develop as a result of the interaction of employees with security controls, such as passwords, passcards, or antivirus software. An information security culture is a way things are done in the organization to protect information assets (Da Veiga, 2015). Kraemer, Carayon and Clem (2009) point out that the security culture perspective is multidimensional, including security governance, control, coordination, security processes, management support, employee participation and training, and employee safety awareness. By assessing the range of information security dimensions, it is observed that the educational issue of the employee with regard to information security should be referenced not only in the business environment but also as regards the behaviour of this person outside the organization (Da Veiga, 2015).

For this reason, citizens' training is paramount for conscious attitudes towards security incidents, regardless of the corporate or social environment. According to Workmann (2007), when the act of perception occurs internally, actions and reactions can be changed, and in this case, the instrument that promotes change is persuasive communication. For this reason, the persuasion factor determines the behaviour of people in situations of threat. Regarding developments in persuasion, there are three emerging factors: trust, fear and commitment. Several attacks take place when potential Attackers use the acceptance of a particular message with the user through elements such as credibility, friendliness, or any appeal to the sender of the message, that is, they use a peripheral persuasion route. There are some characteristics that are linked to the peripheral persuasion route and can be described as reciprocity (normative commitment), consistency (continuity commitment), social proof (effective commitment), sympathy (confidence building), authority (fear generation) and scarcity (perceived lack of certain Items) (Workmann, 2007).
In addition to looking for signs of adverse behaviour on potential attackers, concern about actual attacks must always be maintained. This involves a combination of procedural, people management and performance measures across all those under a manager's mandate, including outsourced employees. This stance leads to a closer relationship between security requirements and the overall business. It is believed in an active approach to the detriment of reactive in both elements, managers and employees. The focus is not just on collecting different data on anomalous behaviour, but also on collecting and analyzing data that can determine the patterns and courses of corrective measures (Colwill, 2009).

It is assumed that the threat to insider information and information security cannot be completely eliminated 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.

Final Considerations

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 and information security from the perspective 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 information technology departments drive many information security initiatives, the real reasons for the failures continue to permeate 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 an effective and efficient information security management.

Acknowledgement
This article is financially supported by:
1. Faculty of Information Management, UiTM Selangor, Malaysia

Corresponding Author: Norhayati Hussin. Faculty of Information Management, Universiti Teknologi MARA (UiTM) Selangor, Malaysia. Email: yatihussin@uitm.edu.my

References

Aronovish, A. (2018). Why Educating Your Employees on Cyber Intelligence And Security Will Reduce Risk. Retrieved April 2020, from: https://www.cybintsolutions.com/employee-education-reduces-risk/

Allen, B. L. (1996). *Toward a user-centered approach to information systems*. Los Angeles: Academic Press.

Alevriadou, A., & Massi, M. (2013). An Intervention Program Related to Reading Development – A Case Study of a Child with Williams Syndrome. Multilingual Academic Journal of Education and Social Sciences, 1(1), 86–100.

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. (2010). MS ISO/IEC 27001:2007 Information Security Management System (ISMS) Implementation, ed. Malaysia: Cyber Security Malaysia

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/S1754-4548(08)70149-9

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

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. (1998). Digital Library Research and Development. *Encyclopedia of Library and Information Science*, 63, 611-19

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. (2006b). Revisiting user studies and information needs. *Journal of Documentation*, 62, 680-684

Fenz, S., Neubauer, T., Accorsi, R., Koslowski, T., (2013). Forisk: formalizing information security risk and compliance management. In: *43rd. Annual IEEE/IFIP Conference on Dependable System and Network Workshop*, 1-4. Retrieved April 2020, from: https://ieeexplore.ieee.org/document/6615533

Harib, A. R. H., Sarijan, S., & Hussin, N. (2017). Information security challenges: a malaysian context. *International Journal of Academic Research in Business and Social Sciences*, 7(9), 2222-6990.

Tarun, R. (2018). A Layered Approach to Cybersecurity: People, Processes, and Technology. Interconnecting Business and Cybersecurity. Retrieved April 2020, from: https://www.csoonline.com/article/3326301/a-layered-approach-to-cybersecurity-people-processes-and-technology.html

Kadir, M. R. A., Johari, N. I. S., & Hussin, N. (2018). Information Needs and Information Seeking Behaviour: A Case Study on Students in Private University Library. *International Journal of Academic Research in Progressive Education and Development*, 7(3), 226–235.