CONSIDERATIONS REGARDING THE INCLUSION OF CYBERSECURITY IN KNOWLEDGE MANAGEMENT

Andrei ȘANDOR, Gabriela TONT

University of Oradea, Romania
andrei.sh@protonmail.com, gabriela@gabrielatont.com

Abstract: *The development of information and communication technology brought many advantages to management and especially to knowledge management. Despite of this fact, it also brought vulnerabilities, threats and risks regarding the security of the information and organizational knowledge capital, that can conduct to information and knowledge theft. Therefore, organizations must find solutions to use technology in an efficient and secure way, considering cybersecurity as an important part of its knowledge management strategy. Even if we should be tempted to consider that cybersecurity is related just to technology, it has a much wider field of application and can have a good impact also on the other two knowledge management components: people and processes.*

Keywords: knowledge management, cybersecurity, information, technology

1. Introduction

Cybersecurity is a wide used term, with multiple definitions, all of them referring to the security of the cyberspace. Cybersecurity includes the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from the facto property rights [1]. Even if it is usually related to use of systems and Internet, cyberspace is more than the Internet, including not only hardware, software and information systems, but also people and social interaction within these networks [2]. The approach of cybersecurity from a KM (Knowledge Management) perspective was chosen because knowledge management covers most of the processes in modern organizations that involve the use of data, information and knowledge in a broad framework. Also, knowledge management is the discipline responsible for managing the organization's knowledge capital, which also includes its protection. This is

important for any organization because protected knowledge may represent a competitive or strategic advantage on its field of activity. Therefore, knowledge is a very important factor that can multiply the capabilities of an organization, often being associated with power.

2. Literature review

There are few studies regarding cybersecurity in knowledge management or how knowledge management can improve cybersecurity in organizations. However, even if cybersecurity is not considered a knowledge management issue, the role it should play in cybersecurity is significant [3]. Knowledge management tools can be used to evolve newer, economical and faster methods to deal with information security issues [4]. This tools may include knowledge management systems with machine learning capabilities and artificial intelligence. Artificial intelligence systems could encode knowledge about cyber-attacks

and knowledge management techniques can distribute that knowledge effectively to address vulnerabilities [5]. Besides complex knowledge management systems, there may be used also simpler tools to promote knowledge management principles in any domain as knowledge protection includes juridical, strategic, organizational and technical components [6].

Knowledge management has also a social and psychological component, highlighted by the culture of the organizations. In the context of information security, security culture decides how much security knowledge is disseminated within the community and what knowledge learners can learn [7]. Like information flows, knowledge sharing, and knowledge transfer operations must also enforce access control and security policies [8]. This may be the case of organizations that own sensitive knowledge, like intelligence or military bodies. In more transparent organizations, there appears another knowledge management issue, regarding knowledge transfer. Security information lies scattered throughout the organization, knowledge creation and diffusion remain an ad hoc process and tacit knowledge of security experts is in most cases preserved as their personal property [9]. This shows a characteristic of the security-related knowledge, namely that is difficult to transfer and oriented towards the tacit dimension of knowledge.

3. Methodology

Having established that generally security and particularly cybersecurity has certain connections with knowledge management, we will go further and analyze if cybersecurity could be included in knowledge management. Therefore, the following hypotheses are formulated:

H 1: cybersecurity can protect knowledge management components

H 2: knowledge management includes cybersecurity

In order to show that the statements are true, during the following chapters there will be presented some aspects regarding the vulnerabilities, threats and risks from the cyber environment that target knowledge management components and how cybersecurity can reduce these issues.

In order to better analyze how cybersecurity can intervene in knowledge management, we will divide the second domain into its main components: people, processes and technology. This way, we can better observe some gaps in security that could be exploited by hackers or other malicious entities and how they can be filled by cybersecurity if discovered at the right time. In the end, using a generalized inductive reasoning, there will be shown that if the main parts of a system, in our case – people, processes and technology include a cybersecurity component, then the entire system, in our case – knowledge management, should also include a cybersecurity component.

4. Personnel awareness and education

People are important in knowledge management for several reasons. First, they offer the organization a unique identity through the organizational culture that can promote desirable values among its members. Secondly, KM mechanisms are human based solutions which are used with IT for implementation of KM [10]. Another reason why the human component is important in KM is noticed by Nonaka [11], who claims that new knowledge always begins with the individual, idea that is also supported by the social constructivism theory.

People can store and transfer knowledge, and therefore they may be a target for malicious entities just like information systems. More than that, according to Badea-Mihalcea, the human factor represents the weakest link when ensuring the network security and this is due to lack of basic cyber hygiene [12]. Other reasons for which people can be targeted in the cyber environment is because humans are

more likely to make errors than computers and it is easier to trick a human than break into a computer or server. This is why cybersecurity should include the human component in any strategy that aims the protection of the knowledge capital of any organization.

The lack of basic cyber hygiene is a result of a reduced cybersecurity culture. This happens when people do not realize the importance of the knowledge they hold, so they do not care too much about privacy and data protection. People's way of thinking can be influenced if organizations adopt some strategies, that must include education.

Through appropriate education on cybersecurity matters, organizations can better protect the knowledge and information held by its members and make them more resilient to cyber-attacks, social engineering or other malicious activities conducted in the cyber environment.

Knowledge management should consider education and cyber awareness as a continuous process of knowledge transfer, permanently adapted to the modern vulnerabilities, threats and risks. The educational process should be guided on the following directions: best practices when using information systems, knowledge of cyber-attack vectors, protection means against malicious software or cyber-attacks and not at least, adoption of a secure behavior when using social media. All these topics should be presented in an appropriate way, correlated with each other and in concordance with the level of understanding and the technical skills of the organization's members.

People should possess some cybersecurity skills because, nowadays, it is not enough to have configured devices and implemented protection means at work, inside the organization's perimeter. This is obvious if we consider the working conditions during the COVID-19 pandemics, when many companies have chosen to work remotely in order to protect its personnel. Also, by living in a media-

saturated social world, we leave behind footprints of our media use [13] and this may expose both personal and organization-related data. This creates some new requirements regarding the use of information devices from both a social and a technical perspective and should expand the scope of knowledge management. Therefore, organizations should consider the knowledge from the cyber dimension – computer skills, cyber communication skills or cybersecurity to be similar to the tacit dimension of knowledge, having in mind that both types of knowledge are stored by individuals.

5. Cybersecurity issues regarding organizational processes

Organizational processes can be considered as a set of activities conducted under a set of both formal and informal rules and workflows. By using specific processes, organizations aim maximum productivity and efficiency. In this article, there will be taken in consideration only the processes that may be the subject of knowledge management. This does not restrict very much the organizational processes we refer to because organizations tend to use knowledge as much as possible, in every aspect of every activity. This can make the organization more productive and efficient, leading to a competitive advantage.

Given the fact that information and knowledge is stored and transmitted through information systems, cybersecurity is present in all processes which implies the use of any communication and information devices or technologies. Knowledge management can improve cybersecurity on its processual component by establishing an adequate framework that enables maximum protection regarding the knowledge capital of an organization. This framework should include rules and best practices that can prevent accidentally loss or theft of information and knowledge.

The main process-related aspects which can improve the security from the cyber domain

in an organization are the following: access control, coverage of information needs, communication security and the existence and application of IT procedures. The first proposes that every member of the organization has specific access rights to information and knowledge, based on job requirements. This should not interfere with the coverage of informational needs, which means that the organization members should be informed and offered knowledge if needed, because otherwise people will search it outside the organization. This includes mainly the existence of a functional communication channel between management and workers. This channel should be protected in the same way as the other communication channels used to transmit or transfer knowledge to or between individuals from an organization. This protection sums up the protection measures that every member of an organization has to respect, such as using secure devices for work-related tasks or keep away personal devices from the work-related network. By having well-defined processes and rules, people are less likely to make mistakes and become victims to cyber-attacks or other activities such as social engineering.

6. The security of knowledge management systems

Knowledge management systems (KMS) are a particular type of systems used by organizations in order to facilitate the creation, storing and transfer of knowledge. According to Becerra-Fernandez and Sabherwal [14], knowledge management systems can be classified as: knowledge application systems, knowledge capture systems, knowledge sharing systems and knowledge discovery systems. This classification is useful because each type of systems has specific particularities which may help us identify relevant aspects regarding their security.

The first type, knowledge application systems, are those type of systems that help

people in their activities by providing knowledge in the desired location and in good time. It includes task management platforms, decision support tools or knowledge-based systems with machine learning and artificial intelligence capabilities. In order to be reliable, these systems should be protected when given input data and when designing algorithms. If the data used by knowledge application systems is not accurate, the output data will not reflect the reality. The solution to this issue can be data filtering, so that the system will get less noise – unwanted or inaccurate data. The other vulnerable point – the algorithm or reasoning mechanism should be protected against unauthorized changes that may affect the system's working capacity through the use of anti-malware software and firewalls.

The second type of systems, the knowledge capture systems, are a category of systems that store information and knowledge into databases that is managed according to a knowledge management strategy. This means that those databases are designed in a way that permits document management and classification of knowledge, has archiving features and included metadata that makes knowledge easier to be found by search engines. The main vulnerabilities, threats and risks against the knowledge capture systems are the same as in the case of any database application: excessive privileges, malware, backup exposure, database vulnerabilities and misconfiguration, denial of service, SQL injections, weak audit trail, weak authentication, unmanaged sensitive data, limited security expertise and education [15]. Most of the vulnerabilities and threats that occur can be reduced by adopting secure programming procedures and by applying updates and security patches.

The third type of systems - knowledge sharing systems, are used mainly in processes that imply the transmission or transfer of knowledge and include email, messaging and voice services, video conference devices,

platforms for collaborative work and so on. The protection of knowledge sharing systems should include access control and encryption. The last type of systems discussed in this paper, the knowledge discovery systems, makes possible the creation of new knowledge. It consists of analysis and statistics systems that may present all the existing data, information and knowledge under a new perspective, facilitating the development of new concepts and ideas that may conduct to new knowledge. Similar to the knowledge application systems, the knowledge discovery systems are dependent on the input data and have similar vulnerabilities. Furthermore, knowledge discovery systems can manage big data, feature offered by its high processing capacity. This can be affected by cyber-attacks such as denial of service, but by using packet filtering and firewalls, organizations can mitigate this kind of attacks.

In order to have fully functional knowledge management systems, organizations should have a good and reliable network because IT's reliability seems to be one of the key factors that influence the organization's competitive advantage from its application to the ability to benefit from IT during the entire innovation process [16]. To maintain a reliable IT infrastructure, organizations should use technology according to a knowledge management strategy and cybersecurity should be part of it in order to create and maintain a secure environment.

7. Conclusions and further discussions

The first hypothesis, according to which cybersecurity can protect knowledge management, can be considered true because cybersecurity measures should and can be met in all knowledge management components. Cybersecurity is implemented

in its technologies and processes, aims people through education and awareness and represents an asset that can be embedded in the organizational culture.

The second hypothesis, which states that knowledge management includes cybersecurity, can also be validated because each of its components – people, processes and technologies contain some elements regarding cybersecurity. So, it is no doubt that if all the components of a system include a domain, the system will also include that domain. Knowledge management strategies should include cybersecurity in order to protect not just its technology, but also the people and the processes from an organization.

This article can offer managers a complementary perspective regarding cybersecurity, as it can be implemented also from a knowledge management perspective. If analyzing cybersecurity from different viewpoints, managers can better identify the vulnerabilities, threats and risks and enhance the protection of the organizational knowledge capital.

Given the fact that technology is more and more present in our lives, we can consider that in the future this trend will be maintained, and cybersecurity will continue to be important for organizations. It should be considered part of knowledge management and promoted through organizational culture, as well as processes and technology. Even if it may be considered a very complex and complicated domain, organizations should find ways to educate its members and promote a secure working environment especially in the cyber domain, that will be more and more important for knowledge creation, transmission, transfer and storage.

References List

- [1] Craigen D., Diakun-Thibault N., Purse R. Defining Cybersecurity. *Technol. Innov. Manag. Rev.* October 2014; 4(10):13-21.

- [2] Klimburg A.(ed). National Cyber Security Framework Manual. Tallin: NATO CCDCOE Publication; 2012.
- [3] Tisdale S.M. Cybersecurity: Challenges from a systems, complexity, knowledge management and business intelligence perspective. IIS. 2015; 16(3):191-198.
- [4] Mittal Y.K., Roy S., Saxena M. Role of Knowledge Management in Enhancing Information Security. IJCSI. November 2010; 7(6):320-324.
- [5] Kingston J. Artificial Intelligence, Knowledge Management and Human Vulnerability. In: Griffiths P., editor. European Conference on the Impact of Artificial Intelligence and Robotics. Oxford: EM-Normandie Business School; 2019. 198-204.
- [6] Grimm M., Anderl R. Intellectual Property Protection and Secure Knowledge Management in Collaborative Systems Engineering. Procedia Comput. Sci. December 2013; 16:571-580.
- [7] Wen S.-F. An Empirical Study on Security Knowledge Sharing and Learning in Open Source Software Communities [Internet]. 1 October 2018 [6 February 2021]. Available from: <https://www.mdpi.com/2073-431X/7/4/49>.
- [8] Bertino E., Khan L.R., Sandhu R., Thuraisingham B. Secure Knowledge Management: Confidentiality, Trust, and Privacy. IEEE Trans. Syst. Man Cybern. A Syst. Hum. May 2006; 36(3):429-438.
- [9] Belsis P., Kokolakis S., Kiounouzis E. Information systems security from a knowledge management perspective, Inform. Manag. Comput. Secur. July 2005; 13(3):189-202.
- [10] Nazaridou M., Bidgoli B. M., & Rezaeenoor J. Providing a Triangular Model for Gap Analysis. Case Study: Iran Khodro Company. IJCSI. January 2013; 10(1):627-638.
- [11] Nonaka I. The Knowledge-Creating Company. Harvard Business Review. July-August 2007. 162-170.
- [12] Badea-Mihalcea A. People and Machines: Dealing with Human Factor in Cyber-Security. In: Mihai I.C., Ciuchi C., Petrica G., Considerations on Challenges and Future Directions in Cybersecurity. Romanian Association for Information Security Assurance; 2019; 143-154.
- [13] Hepp A., Friemel T., & Breiter A. Digital traces in context. Int. J. Commun. January 2018; 12:439-449.
- [14] Becerra-Fernandez I. and Sabherwal R. Knowledge Management: Systems and Processes. New York: M.E. Sharpe; 2014.
- [15] Malik M., Patel T. Database Security – Attacks and Control Methods. IJIST. March 2016; 6(1):175-183.
- [16] Tworek K., Walecka-Jankowska K., Zgrzywa-Ziemak A. IT Reliability and Innovation in SMEs: Empirical Research. J. Manag. Bus. Adm. Cent. Eur. June 2019; 27(2):83-96.