International Journal of Information Management 35 (2015) 154–159

Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt

Advanced techniques for knowledge management and access to strategic information

Lidia Ogiela*

AGH University of Science and Technology, Al. Mickiewicza 30, PL-30-059 Krakow, Poland

ARTICLE INFO

Article history:

Keywords:
Knowledge management
Strategic information
Cryptographic algorithms
Secret sharing

ABSTRACT

This publication discusses advanced knowledge management techniques based on information splitting and sharing algorithms for secret, strategic information. Information splitting techniques will be dedicated to problems of secure information storage and managing sets of strategic data. The management of strategic corporate/organisational data will provide the illustration of the discussion of knowledge management which constitutes the starting point for advanced information management processes. Advanced knowledge management techniques will be discussed using the example of applying cryptographic algorithms in processes of managing information and access to it. Restricted access to strategic corporate information means that this type of data must be stored securely and must not be disclosed to unauthorised individuals. The use of cryptographic algorithms for strategic information sharing keeps this data completely confidential and ensures no access of unauthorised people to the knowledge possessed.

1. Introduction

Knowledge management is a very difficult task in the contemporary world. This is because it poses challenges concerning the correct management and is considered to be one of the most difficult of all currently known management problems (Laudon & Laudon, 2002; Ogiela, 2013a). What is this difficulty about? Firstly, it relates to defining what knowledge really is, in precise terms. In addition difficulties as seen in the way of using knowledge as well as the intentions and methods of using it. When knowledge is used for cognitive, scientific, interpretation purposes, it is easy to define and identify (Bodzioch & Ogiela, 2009; Hachaj & Ogiela, 2011; Ogiela & Ogiela, 2012a; Ogiela, 2008a, 2008b, 2008c). However, when it is used for unethical purposes, it becomes difficult to define and it is difficult to confirm that this or that layer of knowledge was used. In this case, an ethical contradiction arises: knowledge which is perceived as an element of the ethical world can be used for unethical purposes. It is, therefore, important what purpose information, data and messages constituting elements of the knowledge are used for, who uses the collected knowledge and what for, whom the results of the use knowledge concern, etc.

It is very similar with regard to identifying, defining, and sourcing knowledge in an organization (Buchanan & McMenemy, 2012; Ogiela, 2013a; TalebiFard & Leung, 2011). How to collect knowledge, how to use the collected knowledge, in what case to use it, etc.: decision-makers are constantly struggling with these and similar questions. However, answering these questions does not yet guarantee that the organisation will operate correctly. It is only the efficient management of knowledge collected within the organisation that guarantees the correct growth of the company. In management processes, knowledge is understood as the correct use of all reliable information about the past, present and future situation of the company, its environment, the reasons for the current situation and also the ability to project the future state. Knowledge accumulated at various levels allows management processes to be improved, but only that collected at the highest level, i.e. the strategic decision-making one, allows the organisation to be managed effectively because it enables the intellectual capital of the organisation to be consolidated. Just collecting knowledge is obviously insufficient, what is important in knowledge management processes is using it properly. IT systems for knowledge management which improve management processes differ depending on whether the knowledge is centralised or decentralised. In every system, however, it is important that information should be transferred efficiently and reliably. If information is distorted or omitted, the entire knowledge management process becomes useless (Bernstein & Wild, 1999; Ogiela & Ogiela, 2011; Ogiela, 2013b, 2013c).

In traditional knowledge management systems, layers of information form an element supporting corporate management. This situation is presented in Fig. 1.

* Tel.: +48 12 617 45 07.
E-mail address: logiela@agh.edu.pl

http://dx.doi.org/10.1016/j.ijinfomgt.2014.11.006
0268-4012/

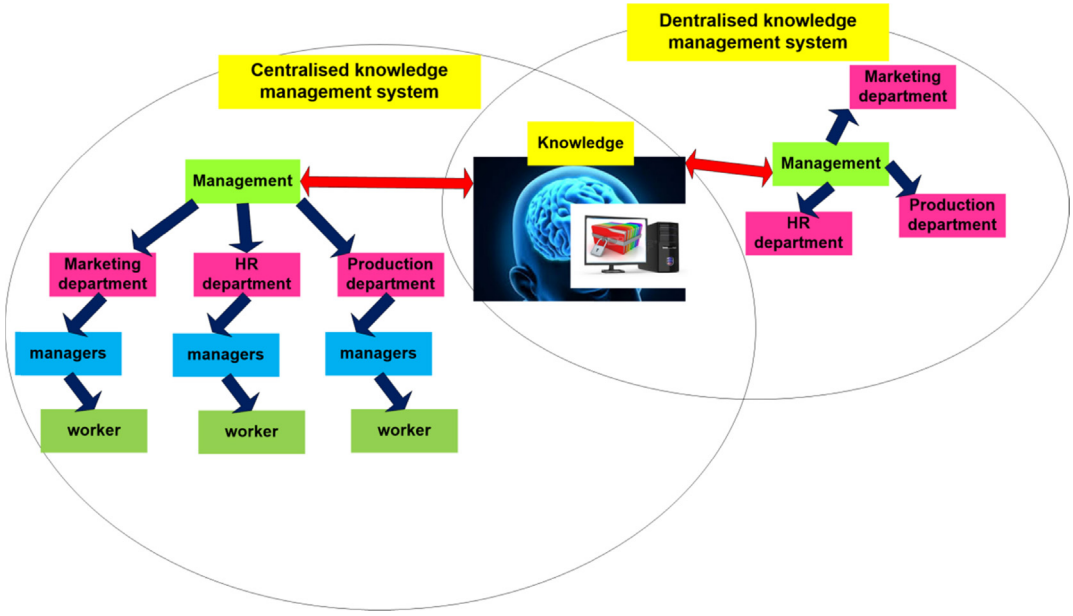

Fig. 1. Knowledge layers in knowledge management systems.

In both cases, managers gain the most accurate knowledge possible in order to collect the complete information about the company situation, its environment, competitive conditions, the drivers of the current and future company success, the reasons for its failure, etc. There are, however, differences in how knowledge is transferred between the remaining elements of the entire system. These differences are mainly due to the design and type of organisational structures to which they are dedicated.

In a centralised system, knowledge forms one of many elements of the entire management process, whereas in a decentralised one, it constitutes one of few elements of the entire system. Consequently, in knowledge transferring processes, it is better to use decentralised systems as they pose a lower risk of possible distortions or errors at each stage of knowledge transfer.

Knowledge management processes do not apply solely to the methods of collecting knowledge, processing it and using it to improve the operational processes of the organization. Obtaining knowledge from generally accessible information resources implies the use of information management processes including the following topics (Ogiela & Ogiela, 2014):

- planning, designing and implementing an information strategy;
- the information flow in external communication;
- the information flow in internal communication;
- ensuring investment funds for developing and implementing new IT solutions;
- the correct use of available IT solutions;
- information quality management;
- ensuring data security;
- ensuring training and development of the IT staff and system users;
- the ability of the company to effectively interact with the information market;
- integrating information systems used at various levels.

Information management processes precisely indicate directions in which knowledge management process support will be used to secure strategic information. The analysis of this subject forms the basis of this work, and the related methods will be discussed in subsequent chapters.

2. Cryptographic algorithms for strategic data division

The correct, i.e., secure, process of managing knowledge within a business organisation/enterprise/company can be ensured by using cryptographic information division algorithms in such a way that company security is entrusted not to one person but to a certain trusted group. Such capabilities are offered by cryptographic algorithms which divide information. These protocols are used to divide information within a given group of secret trustees. The secret consists in secret, strategic information which must not be disclosed publicly. The trustee can be either a person or a computer. The data division algorithm is used to divide this data (depending on the cryptographic algorithm applied) within a selected group of secrets trustees. In the information division process, security must be ensured:

- during the allocation of shares of the secret to each of their holders;
- at the stage when these holders store their shares; and
- at the stage when these shares are combined to recreate the split information.

Data division techniques are classified into two basic groups.

The first comprises information splitting algorithms, designed for splitting information into shares, which are distributed to all secrets trustees. Each trustee receives their share of the split secret, and all shares must be combined to recreate the split information. The lack of even only one share makes it impossible to recreate the original information.

The second group comprises data sharing algorithms. This type of algorithm is used to divide information within a selected group of secret trustees, each of whom receives their share of the divided secret. However, to recreate the divided information, it is necessary to combine a number of secret shares (which number is selected when the algorithm is defined).

Information sharing protocols enable any data division between n protocol participants. Theoretical foundations of data sharing algorithms are described, among others, by (Menezes, van Oorschot, & Vanstone, 2001; Ogiela & Ogiela, 2014; Schneier, 1996; Shamir, 1979; Tang, 2004):