

The need of knowledge management for the security management

Oldřich LUŇÁČEK

Dept. of Communication and information systems, University of Defence, Kounicova 65, 662 10, Brno, Czech Republic
oldrich.lunacek@unob.cz

Abstract. *The aim of this article is to perform an analysis of the information resources in support of activities of security management. The current situation is marked by information overload, which can cause confusion. It is imperative to identify information sources and then sort. Aspects for sorting sources may be different and therefore it is proper to compare them and select the one that most affects the solved area. Persons holding management roles in the security they need to support their decisions adequate information support.*

Keywords

Information, Protection, Security, Support, Secrecy

1. Introduction

The area of security of information is very sensitive part of the each organization. It is necessary to solve topic which is called security triad. Security triad means technology, personnel and legislative. Especially parts of personnel and legislative are very important. Only prepared personnel can use sophisticated technology in environment which is described in information sources.

2. Information

Information can generally be defined as information, communication, message, which enriches us as a recipient of information. Information is sometimes referred to as the data. The use of the term varies with regard to discipline. It can be concluded that the information removed the uncertainty; it is an answer to the question. In view of the human being, we can assess the information on the following properties:

- The truth - this is the need for a definition of truth, but also false. False information is in error, mistake or disturbance, and thus inadvertently, or deliberate lies.

- Timeliness - the property information, where the recipient gets information before or at the time when it is needed.
- Relevance - this is the relationship of information to the problem addressed.
- Completeness - there is a relationship to readability (interpretation) of information.
- Clarity - this term is marked as compatibility (language and conceptual clarity).
- Redundancy - this term addresses the redundancy information.

We can use other criteria's like accessibility, completeness, etc. For the storage of information (data) we use media. Media can be divided into electronic and non-electronic. Today, it is mainly the storage of information on computer media, which include magnetic media, optical media, and electric media. It should be noted that an electronic record of the information (data) is gaining importance.

3. Information society

After clarification of information environment, it is important to recall the role played by information in human society. Human society is undergoing development and today's information society is continuing development of the company after the industrial society. Scientific and technical discoveries led to the industrialization of society and to improve the standard of living. Particularly in areas such as electrical engineering, computer science and communications have brought us very changes which affected the normal life and society. Society's character has changed, because information and communication technologies (ICT) to supplement the resources (raw materials, energy, capital and people) required for the development and operation of the society. The society is forced to react and try to edit the information environment in order to regulate or restrict the information environment. The changes have brought us unfamiliar type

of crime, like piracy, cyber crime, such as hacker attacks, etc. ICT contributes on the globalization of the world and has contributed to the repeal of time-spatial barriers. It has a negative but a positive knowledge. In this information age comes to the confusion of the information environment, owing to the amount of information, truthfulness, usefulness, or redundancy.

4. Information resources

For clarification of the information environment is necessary these information sources to gather, collate and present knowledge. Way to do that may be deployment of information systems, which have the task of systematically integrate downstream and overlapping information sources and provide a summary and the "condensed" knowledge. We must specify the basic information resource that is the source, consisting of media and a set of data or information, which are in a medium fixed and formally organized and content. If we apply the division of information resources by Vymětal [1], we have made the division into four groups:

- primary,
- secondary,
- tertiary,
- other.

Generally, the distribution of the information will be as follows general and simple information obtained from textbooks (tertiary information source) has its basis in an external corporate information (secondary information source), and this was based on standards as a primary source of information. These categories differ, spreading, but also the accuracy of the details.

5. Security management

For the success of the organization is a key figure the security management, in particular to meet tasks in the area of the protection of information. The security personnel decide, and implement effective protection of information. We can estimate that the demands on the important positions should be laid. But the reality is different, because no limit and conditions have been set. Only personal security clearance is required for these persons. The requirement for these persons should be so high, the management should be professionally ready especially for controlling and planning, and able to choose and subsequently lead the security of the organization. Monitoring and evaluation of the profile of persons for the security management is so very important. These persons may come into contact with sensitive data, personal information or classified documents. The structure, built on a hierarchy of subordination and direct individual entities used the principle of the use of obligatory decisions and is capable of rapid response to security incidents. Security management is responsible for making decisions and for the implementation

of the protection of classified information by following kinds of reinsurance:

- personnel security,
- physical security,
- administrative security,
- security of information and communication systems,
- cryptographic protection,
- industrial safety.

The organization during wide spectrum of all activities will come into contact with a lot of information. It is necessary to establish very effective system for the control of information flow. The main point should be security management with security manager in head. It must be clear if the information needs some kind of protection or not. The distribution of information can be described:

- Classified information (protected by Law No 412/2005 Coll)
 - Top Secret,
 - Secret,
 - Confidential,
 - Restricted.
- Non- classified information
 - Non-publicly information (is not subject to protection),
 - Information. to which the covered by the obligation of secrecy (tax, criminal proceedings, etc.),
 - Personal information (protected by Law No 101/2000 Coll),
 - Special facts (Protected by Law No 240/2000 Coll).

6. Information support of the security management

If we are assuming that security management is primarily intended for the protection of classified information, we need to focus our attention on the sources of information for the regulating the area of classified information. According the above mentioned division of information we will use the division which is done by Vymětal. The division respects the hierarchy of the sources and it will help us to understand wide spectrum of the sources and their relations. The possible division of information resources is as follows:

- Primary (Laws, corporate, reports, research and technical reports, scientific and technical, professional magazines, etc.)
- Secondary (Secondary literature, compendium, magazines, literature citations, etc.)
- Tertiary (Corporate publications, manual, monograph, dictionaries, textbooks, etc.)
- Other (Translations, catalogues, lists of authors, lists of periodicals, etc)

In the category of information sources that deal with the protection of classified information sources we have to work with publicly accessible and sources not publicly accessible and they are subject to classification. Classified information, according to the possible injury to the disclosure or abuse is divided into four categories according to the degree of classification Top secret, Secret, Confidential and Restricted. Access to classified information is based on the principle of "need to know", when the limited access of only authorized persons should have access to the information. They need for the access to classified information for their service activities. It is desirable, that the system was rational in terms of determining the number of persons and in terms of the classification of classified information. In general, the document of the higher law force must be respected by the document of the lower legal force document. Lower legal force document may the conditions do stricter but never to negate a higher legal standard. If we go through the sources which are valid in the Czech Republic for the area of the protection of classified information we find out a lot of sources. The possible division of the information sources for the area of protection of the classified information is as follows:

- Primary (laws)
- Secondary (the legal implementing provisions issued by the National security authority and the Regulation of the Government of the Czech Republic),
- Tertiary (directives of the individual departments or companies),
- Other (international agreements and documents of NATO and the EU).

7. Way ahead

For the activities of the organization, it is necessary to define the security management, means that will be used for the protection of the information. These persons must be professionally ready for the performance of its functions. For the preparation and for the practice in the area of protection of information is necessary to identify the sources. But the situation is not clear due to the redundancy of the information sources. It is very easy to make mistake, and any mistake should have very important negative consequences. We must be aware that violation of law is punishable. For better understanding is very useful to deal with knowledge management. Knowledge management is the part of the management, whose scope is very wide, implying its nationwide implementation. Everywhere, working with data, information and knowledge, and therefore their management is needed. It is absolutely essential to understand these terms, as they are the basis for knowledge management. Information and communication technologies are an indispensable element for the management of knowledge capable

of harnessing the potential of the knowledge management. Without the technology would not be possible to achieve effective knowledge management. The organization that implements the knowledge system has an advantage. Management of the knowledge management system necessarily requires considerable effort and overcoming many problems especially in the attitudes of people and their integration into the life of the whole system of the organization. The staff must be motivated for usage of new knowledge, and also to share their experience. Problems of the functioning and non-functioning of the system occur throughout the life cycle of the system. Effective knowledge sharing, changes in organizational culture, new management practices, commitment of the top management and technical support must be integrated into the organizational culture. Organization can obtain by implementation of the knowledge management within the organization a number of advantages:

- constraints for loss of intellectual capital in the event that people leaving the organization,
- reducing the costs incurred to repeated the same problem solution,
- reducing the redundancy of knowledge in the knowledge base,
- increase productivity by accelerating the decision-making process,
- increase the prestige of the organization.

Acknowledgements

The article is prepared as a component of the research project for the Development of the CIS Department, Faculty of Military Technologies, and University of Defence. It introduces some outcomes of the solutions in Command and Control Information Systems (C2IS) and Knowledge Management Systems (KMS). Our results are part of the education process within the University of Defence, Brno.

References

- [1] VYMĚTAL, Jan. Informační zdroje v odborné literatuře. Vyd. 1. Praha: Wolters Kluwer Česká republika, 2010, 433 s. ISBN 978-80-7357-520-5. [in Czech]
- [2] FRYŠAR, Miroslav a kolektiv. Bezpečnost pro manažery podnikatele a politiky. Praha: Public History ve spolupráci s Českou asociací bezpečnostních manažerů, 2006. ISBN 978-808-6445-229.
- [3] BUŘITA, Ladislav. Informační podpora v resortu obrany. 1. vyd. Redaktor Jaroslav Furfánek. Praha: Ministerstvo obrany České republiky - Agentura vojenských informací a služeb, 2006, 150 s. ISBN 80-727-8375-0. [in Czech]
- [4] BUŘITA, Ladislav. Informační věk, informační společnost a vojenství. 1. vyd. Praha: Ministerstvo obrany České republiky –

Agentura vojenských informací a služeb, 2007, 141 s. ISBN 978-80-7278-379-3. [in Czech]

[5] LUŇÁČEK, Oldřich. „Integrované řízení bezpečnosti organizace.“
Disertační práce, Univerzita obrany, Brno, září 2010. [in Czech]

About Author...

Oldrich LUNACEK was born in 1966. He received his Ph.D. from the University of Defense in 2010. His research interests include security of classified information and security management.