KNOWLEDGE MANAGEMENT IN INFORMATION SECURITY

Oldrich LUNACEK

[1] Dept. of communication and information systems, University of defense, Street Kounicova 65, 662 10, Czech Republic
oldrich.lunacek@unob.cz

Abstract. *This article discusses the possibilities of application of methodology for integrated safety management of classified information. Systematic work of many staff security management organization is marked by a huge amount of information processed. This information is of different nature and requires a different kind of treatment. Information must be used efficiently and on time. Information must be assessed comprehensively and adequately must also be evaluated. Today's information overload rather difficult decision of responsible persons, and therefore the application of the methodology appear as an appropriate tool for the effective and rational management and dissemination of information. Information is systematically collected and evaluated and then the information can be used in knowledge bases. Knowledge management is also important from the perspective of how to look at the issue and how to express it rationally.*

Keywords

Information, information protection, integrated management, security management

1. Introduction

Currently used methods for information security management is not appropriate for the concept of integrated management of the security. It is due to their universality, or too specific focus. Moreover, mostly based on experience that is more empirical in nature. The current level of knowledge but also offers new approaches for information security management. May be safety mathematization, security classification schemes, optimization methods and increasingly knowledge-based approach used in the processing issues. In this contribution I will focus on clarifying the design methodologies, which will be suitable for the design and evaluation of information security. The proposed methodology respects the concept of integrated safety management. This methodology may become an appropriate tool for security management personnel.

2. Proposal of the methodology for control of the security

Safety means special importance for the organization. Decisions are made here about the success or failure of the organization. Very sensitive part of the security organization is protection of information. According to the type of information is important to distinguish the information for the organization or its partners. Special category is classified information, requiring compliance with the conditions laid down by legislation. Organizations that want to handle classified information must meet strict legal requirements. Ensuring access to such information, the organization is financially costly, and therefore must be managed as efficiently as possible safety. Organizations must develop tools for safety management to be better and more complex. Organizations must build, manage and continuously improve security in a way that is proportionate, consistent and complete.

Integrated security management must be conducted on the basis of the methodology to be complete in all respects and does not depend on the subjective view of the processor and its practical experience. The methodology must cover all areas of protection of classified information. When processing methodology must take into account the requirements:

- the principle of rationality (cost equivalent to the value of protected information),
- the principle of integration (activities in the field of a protected interest must take into account the impacts on other protected interests),
- the principle of "need to know" (rationally apply the disclosure system in the sense that they know only by authorized persons),
- the precautionary principle (since prevention is cheaper than remedial action),
- the principle of synergy (if the variant solutions are possible, it would be preferred such an option which is optimal from the perspective of strategy and available resources),

- the principle of subsidiarity (the problems to be resolved at the lowest possible level - the creation of methodologies for different types of safeguarding classified information),
- the principle of openness and transparency (documents, decisions and their rationale are available to the public professional),
- principle of precision (based on a documented, measurable and controllable tasks and measures).

3. The structure of the methodology

For production methodology, I select an approach where the situation is not dealt with in isolation, all parts are covered, nothing remained underestimated, the corresponding things corresponding meaning, different areas overlap. Based on the analysis on possible new approaches to address issues of integrated safety management organization, I chose the following form processing.

The proposed structure of an integrated methodology for information security management is in the form of a structured questionnaire. The structure and content of the questionnaire is the result of previous analysis of security issues. Its structure recalls the standard NIST SP 800-55-rev1, this standard but only deals with problems of intensive information systems security. In developing the methodology I came also from studies of this issue of knowledge management and especially knowledge hierarchy. When processing methodology, I respect the issue of audit and classification. It should be noted that, especially knowledge management is gaining importance and becoming more and more promoted in various sectors. We analyze the NIST standard and when compared with the problems of knowledge management, realize the similarity of the knowledge hierarchy and NIST standards.

Definition of the measures that we want to address is the first step. The presented methodology is divided into 13 steps which must be positively resolved:

- Planning and financing of security - in the long term it is necessary that all the processes and funds had been planned in the medium term with care and not just on the basis of operational needs. Because resources are limited, it must be rationally used.
- Security management - the strategic part of the management of the organization, which is directly responsible for the security organization. In particular, its performance depends on whether the organization will succeed or not.
- Preparation of human resources - training of human resources is essential in terms of their readiness to respond to change. It is necessary to have the theoretical education, but it is also necessary to prepare a person to practice in real conditions. This includes training for a specific function, and the readiness to use the latest technology.
- Logistics and repair - any technical means to work correctly needs adequate service and if the situation so requires much-needed correction. Adequate logistics security, we save resources.
- Personnel security - only authorized persons have access to classified information, this area affects everyone who wants to have access to information.
- Physical security - classified information must be stored or operated in accordance with applicable legislation, physical security is one of the means to unauthorized access to information to prevent.
- ICS (information and communication systems) security in todays globalized world, it is apparent deployment of information and communication technologies that blur the temporal and spatial barriers. Classified information is mostly stored and transmitted through the ICS and therefore considers this area as very important and watch the information handled in ICS.
- Administrative security - serves primarily to ensure that classified information to authorized persons have access, and to be kept clear evidence about who to that information at that time had access.
- Industrial safety - to enter the field of many companies and suppliers is essential that even these bodies have the information after meeting conditions, access, and to implement course of business.
- Cryptographic protection - classified information is necessary to protect especially when using ICS and through the use of certified cryptographic devices.
- Audit and accountability - audit is an effective tool for the organization. Therefore, the organization can assess how the resources entrusted to be treated, whether the investments are used efficiently, and can assess what is the utilization of individual persons. With the audit we found it easier to remove duplicates.
- Certification, accreditation - many workplaces or equipment must be put into service before examined whether it actually met the conditions of certification and accreditation. These procedures must be performed only by authorized entities
- Plan for emergencies - the organization must be prepared for the creation of exceptional and emergency conditions, and must be able to these situations.

After clarifying the identification of measures is necessary to establish the structure of each measure. After

careful analysis, I chose the following procedure, first were laid down the key points, they are described, then they are asked questions on issues such as point and follow-up is to answer questions. The most important part is the analysis of lessons learned and follow-up. The selected structure is hierarchically organized and comprehensively describes the entire issue. For specialists in each area can be qualified questionnaire in its scope expanded, but the intention is to put the methodology to be able to work with it and use it to control security in their employees along with the methodology to be most effective.

For each proposed structure of the questionnaire measures were established, including the way questions and evaluation. A subsequent step must be to complete a questionnaire designed by a person under particular circumstances. After filling in all the selected measures will collect all the results will be a final report with the presentation of the findings identified. The last step must be acceptance of the findings identified as a security management organization and executive management organization, because only in its promotion will be possible to meet all the requirements arising from the final report.

The structure of the methodology is designed to be given the maximum attention to the fact that the solution to the problem will be addressed in context. To resolve the problem of security, we must work very closely with the information which can be found in the literature. Experience of knowledge management talk about that we should not underestimate the knowledge. The conclusions that we support the methodology, we objectively assess and take appropriate conclusions. On the basis of the results we must take the next step. If we find that the situation meets the needs of not requiring immediate action to change the status quo. However, in the second case, where we find gaps, we must quickly without unnecessary delay, take such countermeasures in order to correct. The result, we get using the proposed methodology gives us an objective picture of how it dealt with safety issues. The final report will contain information that will be exempt from the subjective impression of the processor. The report shall contain the following information with which we work:

- Identification of measures - we need to identify what action we are thinking and what we want to address.
- The measure - which we define the objective we want to achieve and why you want to achieve.
- Reason for the introduction of measures - define why we want to impose measures.
- Consequence measures - we must express the importance and consequences resulting therefore that measure the impact on the organization.
- Expression of measures - how we interpret the result we want.
- Parameter measures - define how we express the objective.
- Evidence of implementation of measures in the organization - it's one of the most important parts of the questionnaire, because it must include an explanation of how the measures we have implemented, how can we realize.
- Evaluation period - who carries out the collection of information - to create different databases and the collection of documents for analysis is necessary to specify in what time frame we will make the collection of information.
- Interested parties - we set who is responsible for tasks, or with whom we cooperate.
- Source of information - for quality processing of the issue is very necessary to have a source of information from which we can draw evidence for action on the basis of what the activity is conducted.
- Expression of the outcome of the action - the appropriate message format will help us to demonstrate the results achieved.
- Type of collateral that has tracked the impact of measures - specifies to which region has the measure actual impact.
- Final evaluation - whether they are satisfied all the requirements under this measure.
- The need for redress - whether it expresses the need to negotiate a remedy or not. Headline of a Section

4. Conclusion

Legislation can not solve all the problems and can not read it all contexts. The methodology is completely focused on the safety of the entire organization and each individual area is divided proportionally but with links pointing to the connection to other parts. Develop methodology may become an appropriate methodological tool for the management of safety both for security management, and for other staff organizations. Result for the practice and especially for the development of science is the systematic verification of safety prepared by the methodology of key management security features, including:

- obtain an objective view of the organization in the field of security,
- report on the state of security, which will include observations on the current condition and indicate what needs to be done in the future,
- monitoring the feedback to learn from the experience and possibly change the priorities in the management,

- identification of needs to create countermeasures in case of impact incident,
- evaluate the system safety organization and
- continuous monitoring, assessment and improve security organizations.

The analysis of results is very important point. Informational value of individual measures will help to better decision making. The quality inputs are critical for a complex analysis of the results and the organization must draw from official materials. The results of the methodology should be grasped for workers who are not specialists in the field of security. These workers should also be able to work with the results occurring processors.

References

[1] GERBER, M., von SOLMS,R. Management of risk in the information age. Computers and Security, January 2005.

[2] FÁBERA, M. Jaká má být bezpečnost. Magazín SECURITY, září/říjen 2007. FAMily media spol. s.r.o. Praha 2007. [in Czech]

[3] SWANSON, M., BARTOL, N., SABATO, J., HASH, H., GRASFFO, L. NIST. Special Publication 800-55 Security Metrics Guide for Information Technology Systems Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8933 July 2003.

[4] ROSS, R., Katzke, S., JOHNSON, A., SWANSON, M., STONEBURGER, G., ROGERS, G. NIST. Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930 December 2007.

[5] STONEBURGER, G.NIST. Special Publication 800-33 Underlying Technical Models for Information Technology Security Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930 December 2001.

[6] CHEW, E., CLAY, A., HASH, J., BARTOL, N., BROWN, A. NIST. Special Publication 800-80 Initial Public Draft Guide for Developing Performance Metrics for Information Security Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930 May 2006

[7] CHEW, E., Marianne SWANSON, M., STINE, K., BARTOL, N., BROWN,A., ROBINSON, W. NIST. Special Publication 800-55 Revision 1 (DRAFT) Performance Measurement Guide for Information Security (DRAFT) Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930 September 2007

[8] BUREŠ, V. Znalostní management a proces jeho zavádění. Grada, Praha 2007. [in Czech]

About Author ...

Oldrich LUNACEK was born in 1966. He received his M.Sc. from the Liptovsky Mikulas Military Academy in 1989. His research interests include security of classified information and security management.