INFORMATION SYSTEMS IN MANAGEMENT

Information Systems in Management (2014) Vol. 3 (2) 134−144

INFORMATION SECURITY MANAGEMENT SYSTEMS IN MARSHAL OFFICES IN POLAND

DOMINIKA LISIAK-FELICKA [a)], MACIEJ SZMIT [b)]

[a)] *Department of Computer Science in Economics,Faculty of Economics and Sociology, University of Łódź*
[b)] *Corporate IT Security Agency,Orange Labs Poland*

The article presents results of a survey concerning Information Security Management Systems (ISMS), which was conducted in Marshal Offices between December 2012 and April 2013. Survey questionnaires were sent to all sixteen Marshal Offices in Poland. The aim of the research was identifying in which government offices information security management systems are implemented, according to which standards are developed and certified and gathering information about factors facilitate the implementation of the ISMS, problems encountered in the implementation of this system and documentation concerning information security.

Keywords: information security, information security management systems, information security policy

1. Introduction

Managing information safety and security [2], [4], [7], [9],[10], [11], [16] in all kinds of organizations is a big challenge for contemporary organizations and institutions.

Information Security Management System (ISMS) is defined in ISO/IEC 27000 standard as part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security (see: 2.23. in [5]). According to the standard scope, the stand-

ard 27k family is applicable to all types of organization (e.g. commercial enterprises, government agencies, non-profit organizations). In the field of research concerns the marshal offices [18].

Particularly interesting, from the point of view of research, a group of organizations that decide to implement the ISMS are public administration offices. First and foremost – as opposed to individual commercial organizations all are forced to various contacts with the administration, and so information security in offices corresponds directly to the security of citizens. Secondly, the government offices have a strictly defined scope of its tasks and competencies, so it is easy to conduct a comparative analysis on information security management in different offices, the role of the "specifics" so important in commercial organizations is minimum in offices [1], [8], [15]. Thirdly, finally – last but not least – offices, in accordance with the principles of the access to public information, are particularly convenient research material, and although the practice shows that the tendency to hide information is present among the workers of offices, however, the responsiveness of research organizational units of public administration is definitely higher than in the case of commercial organizations.

2. Aim of the research

The research had primarily cognitive objective, that was (apart from identifying in which government offices are implemented information security management systems, according to which standards are developed and certified) answer the following questions: the reasons why respondents did decide (or not) to implement and certification of ISMS, how long it took to implement the ISMS, identify problems encountered in the implementation of this system, whether they could count on the support of the state administration bodies, which factors facilitate the implementation of the ISMS, which the operations relating to the operation of the ISMS have the most problems, what documentation concerning information security has been implemented in these units, together with the brief overview of the application, whether the administrator of information security has been appointed, and how often safety reviews has been conducted.

The survey is a part of our investigations concerning selected aspects of cybersecurity in government organizations in Poland [12].

3. Method of the research

The research was conducted using a survey questionnaire. For all marshal offices a letter asking for help in the implementation of a scientific study by completing a questionnaire was sent. The content of the letter was posted a link to the ques-

tionnaire in electronic form, which is located on a server google.com. The annex to the letter with a questionnaire in Microsoft Word file was also sent. In the course of the research numerous telephone and e-mail contacts with officials was conducted.

Obtained 13 positive responses. The Office of the Marshal of Podlaskie Voivodeship sent written notice of the lack of interest to participate in the survey, two offices (The Office of the Marshal of Lower Silesia Voivodeship and the Office of the Marshal of Kuyavian-Pomeranian Voivodeship), despite numerous telephone and email communications from investigator, did not submit any response.

4. Results of the research

Among the 13 marshal offices, in nine the information security management system is implemented. In the four offices (The Office of the Marshal of Lublin Voivodeship, The Office of the Marshal of Łódź Voivodeship, The Office of the Marshal of Silesian Voivodeship, The Office of the Marshal of Świętokrzyskie Voivodeship), such a system does not work and in the past had not been attempts to implement it (see Figure 1).

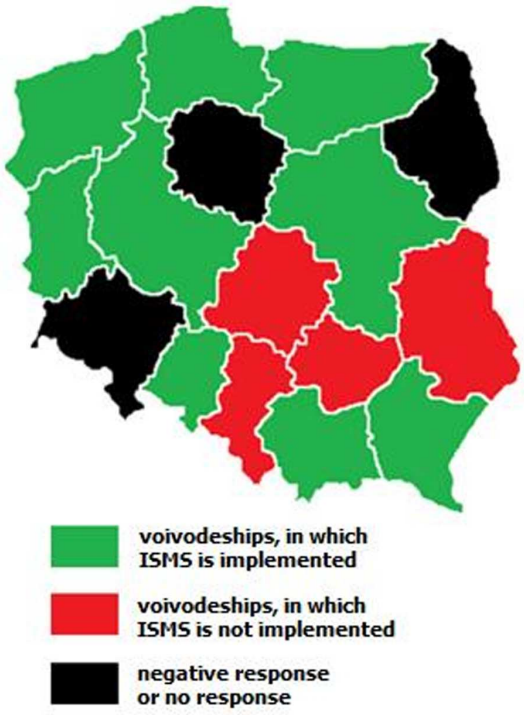

Figure 1. Information security management systems in Marshal Offices

The reasons, why the officials did not take such action, include: lack of funds, lack of time and lack of sufficient knowledge. The reason, why the Marshal Office of the Silesian Voivodeship, was not implemented ISMS is implementation of partial solutions in the field of safety management, which in the opinion of officials are now sufficient due to the nature of the Office.

Seven of the nine implemented Information Security Management Systems – were developed by the recommendations of the standards, including five offices were using PN-ISO/IEC 17799, and two offices ISO/IEC 27002. Detailed answers to the survey questions in this area are presented in Table 1.

Table 1. Development and certification of information security management systems

Voivodeship, in which is the Marshal Office	The system developed by the recommendations of the standards	The system developed by the recommendations of the standards	The system certified compliant with the standard
Lubusz Voivodeship	Yes	ISO/IEC 27002	PN-ISO/IEC 27001
Lesser Poland Voivodeship	Yes	ISO/IEC 27002	PN-ISO/IEC 27001
Masovian Voivodeship	Yes	PN-ISO/IEC 17799	PN-ISO/IEC 27001
Opole Voivodeship	Yes	PN-ISO/IEC 17799	-
Subcarpathian Voivodeship	No	-	-
Pomeranian Voivodeship	Yes	PN-ISO/IEC 17799	-
Warmian-Masurian Voivodeship	Yes	PN-ISO/IEC 17799	-
Greater Poland Voivodeship	No	-	-
West Pomeranian Voivodeship	Yes	PN-ISO/IEC 17799	-

Only in three offices decided to certify the information security management system according to PN-ISO/IEC 27001.

In offices where decided not to certify the ISMS, indicated the following reasons for not taking such action:

- certification does not affect the quality of the information security management (3 answers),
- it is a time-consuming project (2 answers),
- it is an expensive proposition (2 answers).

Respondents from all offices which certify the ISMS said they had decided on this because certification has an impact on the quality of information security management. Also examined the ISMS implementation time. Accordingly, the three offices have identified it as belonging to the range of 6-12 months, one – 12-18 months and four for more than two years.

For the success factors and problems with the implementation of the ISMS [1] respondents indicated respectively, as a source of problems: lack of use of formal methods of implementation of the system (4 answers), lack of substantive preparation workers (3 answers), too extensive documentation (3 answers), insufficient

financial resources (3 answers), lack of experience of the certification body (1 answer).

Only three offices of the nine implementing an Information Security Management System [3] were able to count on the support of the state administration bodies. The stages in which the aid was granted: the establishment information security management system (2 answers), implementation and operation of information security management system (1 answer), monitoring and review of information security management system (2 answers), maintaining and improving information security management system (1 answer), no aid (6 answers).

Only one of the officials showed what this aid consists of:

- The Internal Security Agency and the Inspector General for the Protection of Personal Data supports employees of public administration in the establishment of information security management systems,
- Training own officers and employees, participated in training sessions and conferences organized by other entities,
- Advice and current aid,
- Portals of programs in support the workers on security, guides, explanations, and above all, the database of current legislation and guidelines,
- Visits, audits, inspection, accreditation, certification, etc'.

In another question, the officials indicated which of these factors facilitate the implementation of Information Security Management System. Evaluation factors are shown in Figure 2.

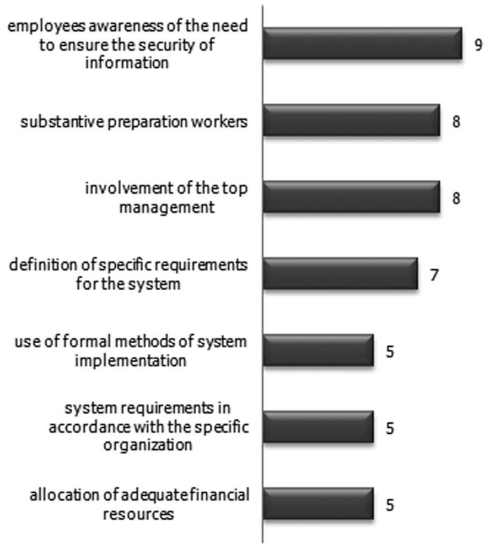

Figure 2. Evaluation of factors that facilitate the implementation of the ISMS

High rating factors: employees awareness of the need to ensure the security of information and involvement of the top management is was highlighted by the comments of an official: ‘The commitment and staff awareness of information security requirements is crucial for the proper functioning of the system. This is achieved by, among others, properly implement the planned course of internal and external training, internal controls, etc.

According to officials, the implementation of Information Security Management System has a positive effect on the unit, especially can increase the level the information security, raising the employees awareness of information security management, is necessary and beneficial. The three officials also indicated that it is an expensive venture (Figure 3).

Figure 3. Opinion on the ISMS implementation

Respondents also indicated the steps on the operation of the Information Security Management System, which have the most problems. The results are shown in Figure 4.

One official also indicated a problem with ‘too frequent regulatory changes and changes in the organizational and staffing (though this is inevitable and should be taken them continuously into account)’. This comment, however, should be included under question concerning problems with the implementation of the system.

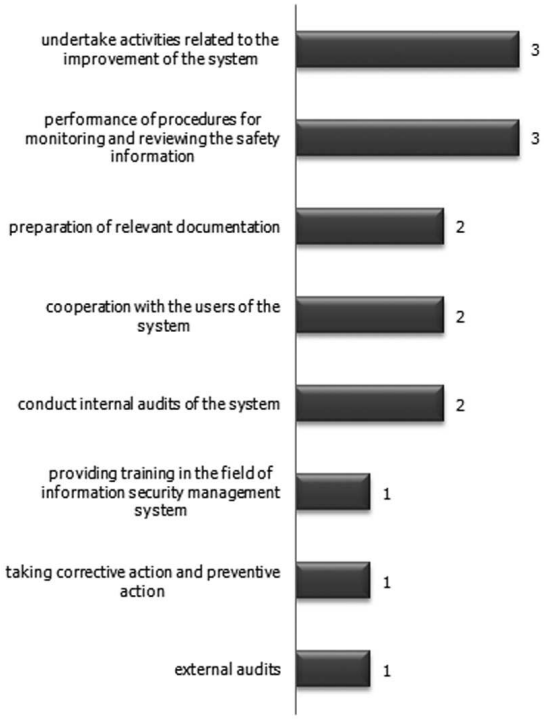

Figure 4. Actions on the operation of the ISMS, which officials have the most problems

Another survey questions focused on conducting documentation. Among the 13 surveyed offices, 12 have developed and implemented an information security policy that contains the policy of protection of personal data in accordance with the requirements of the Law on the Protection of Personal Data [18], [13], [17] and the one of the offices (The Marshal Office of Subcarpathian Voivodeship) has only a policy of protection of personal data in accordance with the requirements of the Law on the Protection of Personal Data [19]. Table 2 presents the characteristics of each document.

Also in each of the 13 units are conducted the security reviews. The frequency of these inspections is shown in Figure 5.

In all of the 13 offices the information security administrators were established and training for employees of the implemented information security policy / protection of personal data policy were conducted.

Table 2. Characteristics of information security documentation in Marshal Offices

Voivodeship, in which is the Marshal Office	Structure	Approximate number of pages	Last updated	Disclosure of document
Lublin Voivodeship	the main document with attachments	102	2012-07-03	Only some parts of the document
Lubusz Voivodeship	the main document with attachments	67	2011-08-16	Yes
Łódź Voivodeship	the main document with attachments	81	2012-06-14	Yes
Lesser Poland Voivodeship	the main document with attachments	50	2012-10-30	Only some parts of the document
Masovian Voivodeship	the main document with attachments	200	2011-12-28 currently being updated	Only some parts of the document
Opole Voivodeship	the main document with attachments	62	2011-06-30	Yes
Subcarpathian Voivodeship	the main document with attachments	43	2012-04-30	Yes
Pomeranian Voivodeship	the main document with attachments	140	2012-04-10	Yes
Silesian Voivodeship	the main document with attachments	110	2012-10	Only some parts of the document
Świętokrzyskie Voivodeship	the main document with attachments	126	currently being updated	Yes
Warmian-Masurian Voivodeship	the main document with attachments	68	2011-11-21	Only some parts of the document
Greater Poland Voivodeship	the main document with attachments	105	2009-08-05 currently being updated	Yes
West Pomeranian Voivodeship	the separate procedures and instructions	about 120	2013-02-22	Yes

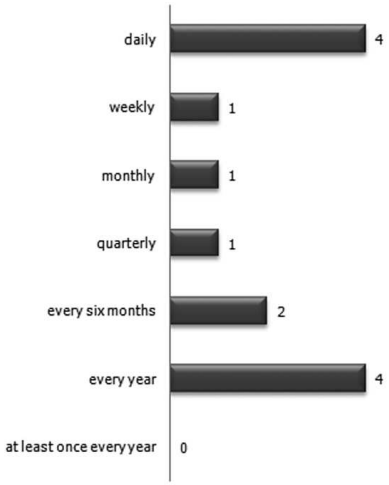

Figure 5. Frequency of the security reviews

5. Conclusion

On the basis on the results of the research it can be concluded, that the issues related to information security are known for officers, especially in the field of personal data protection. All offices have examined the relevant documentation, in each unit the information security administrator was appointed, all units have adequate physical security of access to information and appropriate security systems. Therefore officials are performing tasks in field of personal data protection [14], [19].

In 9 offices, from 13 participating in the research, was implemented information security management systems. The main reasons for which other entities involved in the study did not implement such a system are: lack of funds, lack of sufficient knowledge and lack of time. The first two mentioned tend to be understood. Typically, any action aimed at improving a process at the office, are not made because of the limited budget, or lack of proper training. The last reason is due to poor organization of work and lack of willingness to take on new tasks by the officials.

Based on the responses obtained from the offices in which the information security management systems is implemented, key success factors have been identified to implement the ISMS. These include: employees awareness of the need to ensure the security of information, involvement of the top management, definition of specific requirements for the system, substantive preparation workers.

Therefore, in order to achieve the successful implementation of an ISMS it is necessary to continue raising awareness for employees of all levels of the organization and their respective substantive preparation. This can be achieved through the participation of officials in various training courses in the field of information security. In addition, the subject matter should be addressed in different conferences, involving representatives of the public administration.

Actions on the operation of the ISMS, which officers have the most problems are: taking actions related to the improvement of the system and conducting the procedures for monitoring and maintenance of information security. Only a few offices can count on the support of government units in undertaking activities related to the implementation of the ISMS. It is worth noting the answer to the question on the frequency of ISMS review, which acted as a control question in the survey. Review is an activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives (see: 3.8.2.2. in [6]) (in this case: ISMS) and can be carried out every few months or in the event of need, but it is impossible to review ISMS which has dozens of pages documentation every week or even every day.

Officials also indicate problems they encountered during the implementation of ISMS. In addition to the questionnaire (lack of use of formal methods of imple-

mentation of the system, insufficient financial resources, too extensive documentation, lack of substantive preparation workers) also drew attention to the problems of the legal and organizational nature. The first is a result of frequent changes in rules on information security and inconsistencies of these provisions during the period of change. The second - the frequent organizational changes in personnel offices.

REFERENCES

[1] Calder A.: *Nine Steps to Success: an ISO 27001 Implementation Overview*, IT Governance Publishing, UK, 2005, pp. 107-112.

[2] Gillies A.: *Improving the quality of information security management systems with ISO27000*, TQM Journal, Volume 23, Issue 4, 2011, pp. 367-376.

[3] Humphreys E., Im*plementing the ISO/IEC 27001 Information Security Management System Standard*, Artech House, Norwood 2007, pp. 11-44.

[4] Ilvonen I.: *Information security culture or information safety culture - What do words convey?*, 10th European Conference on Information Warfare and Security 2011, ECIW 2011, Tallinn 2011, pp. 148-154.

[5] International Standard ISO/IEC 27000:2009 Information technology — Security techniques — Information security management systems — Overview and vocabulary. First edition, ISO 2009.

[6] ISO Guide 73 Risk management — Vocabulary. First edition, ISO 2009.

[7] Jašek R.: *The information security of enterprises and citizens' security context*, Komunikacie Volume 7, Issue 3, University of Zilina, Žilina 2005, pp. 45-48.

[8] Kister Ł.: *Significance of information security in a company*, (w:) Riešenie krízových situácií v špecifickom prostredí, University of Zilina, Žilina 2009, pp. 329-334.

[9] Korzeniowski L. F.: Securitology - The concept of safety, Komunikacie, Volume 7, Issue 3, University of Zilina, Žilina 2005, pp. 20-23.

[10] Korzeniowski L. F.: *Informačná bezpečnosť podnikania*. Žilina: Multiprint, 2010

[11] Korzeniowski L. F.: *Podstawy nauk o bezpieczeństwie*, Warszawa: Difin, 2012.

[12] Lisiak-Felicka D., Szmit M.: *"Tango Down" – Some Comments to the Security of Cyberspace of Republic of Poland*, [in:] Biały W. Kaźmierczak J. (ed.), Systems supporting production engineering, pp. 133-145, PKJS, Gliwice 2012, ISBN: 978-83-62652-34-1.

[13] Monarcha-Matlak A.: Obowiązki administracji w komunikacji elektronicznej, Wolters Kluwer Polska, 2008, pp. 239-268.

[14] Regulation of April 29, 2004, by the Minister of Internal Affairs and Administration as regards personal data processing documentation and technical and organizational

conditions which should be fulfilled by devices and computer systems used for personal data processing (Journal of Laws of 2004 No. 100 item 1024).

[15] Robinson N.: *IT excellence starts with governance*, Journal of Investment Compliance, Volume 6 Issue 3, 2005, pp. 45-49.

[16] Stoll M., Breu R.: *Information security measurement roles and responsibilities*, 6th International Joint Conference on Computer, Information and Systems Sciences and Engineering, Lecture Notes in Electrical Engineering, Volume 151, 2013, pp. 11-23.

[17] Suchorzewska A.: *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Wolters Kluwer Polska, 2010, pp. 279-285.

[18] Ustawa z dnia 5 czerwca 1998 r. o samorządzie województwa (Dz. U. z 2001 r., Nr 142, poz. 1590 z późn. zm.).

[19] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 1997 r., Nr 133, poz. 883, z późn. zm.).