SCIENTIFIC REVIEW

MANAGEMENT OF ORGANIZATIONS IN SERBIA FROM THE ASPECT OF THE MATURITY ANALYSIS OF INFORMATION SECURITY

Dragan Trivan ,[8]Olja Arsenijevic [9], Edita Kastratovic[10]

ABSTRACT

The aim of this work is focused on research of information security in organizations, with a focus on cybersecurity. In accordance with the theoretical analysis, the subject of the empirical part of the work is the analysis of information security in Serbia, in order to better understand the information security programs and management structures in organizations in Serbia. The survey covers a variety of industries and discusses how organizations assess, develop, create and support their programs to ensure information security. The survey included 53 companies. The results that were obtained enabled us to select five core elements of the program on the state of information security and cybersecurity in Serbian companies: most companies had not been exposed to cybersecurity incidents; in most companies policy, procedures and spheres of responsibility for information security exist, there are not enough controls to ensure compliance with relevant safety standards by third parties, top management and end-users are insufficiently familiar with cybersecurity risks, although they apply basic measures of protection, safety protection systems are very rare. The scientific goal of this work is to, on the basis of the results obtained, make conclusions that can contribute to the study of corporate information security with special emphasis on cybersecurity. The practical aim of the research is the application of the results for more efficient implementation process of security against cyber attacks in the Serbian organizations.

KEY WORDS: information security, cyber security, cyber attacks, software protection, corporate security

JEL: M15, G14

UDC: 005.52:005.922.1(497.11)
007:004.056]:005

COBISS.SR-ID 227949836

[8]Corresponding author, Faculty of Business Study and Law, „Union – Nikola Tesla“ University, Belgrade, Serbia, e-mail: dragan.trivan@fpsp.edu.rs

[9] Faculty of Business Study and Law, „Union – Nikola Tesla“ University, Belgrade, Serbia

[10] Faculty for Business Economics and Entrepreneurship, Belgrade, Serbia

INTRODUCTION

An organization, as a social system, consists of people who have their own expectations from it. Also the organization's purpose is to provide: personalsatisfaction to its employees and managers, social structure, efficiency, flexibilityand creation of identity(Stojanović et al.,2013,p.75).

The number of incidents in the information security is growing throughout the world, from passive monitoring of announcements to real attacks. Although the data from many studies around the world show that the number of cyber attacks is relatively small, this does not mean that organizations are not at risk. They can have a sense of false security. Taking into account global trends and an increase in the number of attacks, and not to think about cyber security matters, in the end can lead to many Serbian companies become victims of hackers.

THEORETICAL BASICS

Defining of the information protection

Information security is a subject of general interest of the state institutions as well as corporations and other business entities. In this sense, one of the most important tasks is defined by development and implementation of reliable methods and means of information protection, as well as the search for systemic solutions and means of protection, by applying the most effective algorithms and methods of designing means of information protection - instruments of information security (Trivan, 2012,p.88).

Information security is defined as protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transmission, and against the deprivation of services to authorized users, including necessary measures of detection, documentation and elimination of such threats(National Information Systems Security Glossary, NSTISSI No 4009, National Security Agency, Fort Meade MD, September 2000).

Attacks against information systems can be defined as a direct action against the networks and information systems with the aim of unauthorized intercepting or stopping operations, taking control and destroying, changing or corrupting their data (stored or processed).

Rodić and Đorđević(2004,p. 11) suggest that the attackers are the starting point of any attack on a computer system, although they differ in who they are or where they are, according to their abilities and whether they are inside or outside the system they attack. Attackers may be divided into six categories: hackers, spies, terrorists, organized attackers, professional criminals and vandals. The information security measures include the general data protection rules to be implemented at the physical, technical or organizational level. The most important international standard for information security management is ISO / IEC 27001: 2005 and ISO 27001 Standard (Ivandić et al., 2011) .

Although IT sectors are aware of the risks of cyber security, there is no increase of knowledge management in this area (Kolarić et al.,2011).

Relevant research

The e-Crime Report 2011 Managing risk in a changing business and technology environment showed that 25% of organizations in Europe are faced with hacker attacks, viruses and similar problems 10 or more times during the year, that every 5 years one company in Europe suffered significant losses due to damage,that more than 40% of large companies have examples of disclosure of confidential information, and that 20% of companies faced endangering securityof information systems and espionage (KPMG, 2011). Deloitte's did the survey of information security in Central Asia in 2014, with an emphasis on cyber security (DeloitteTSF, 2015). "Kaspersky" laboratory, in cooperation with B2B International, conducted a 2011 survey of information security of business with a focus on current trends in information security of business in Russia. Research has shown that 98% of Russian companies were victims of external aggression, and 82% of internal, and that small and medium-sized businesses lost 780 thousand rubles as a result of these attacks (Kaspersky, 2012). In the last few years, InfoWatch conducts research about the leak of classified information in the world (InfoWatch, 2015). Many studies show that a person is a key factor in information security. He is the creator, the holder, the user and the cause of theft, damage or destruction of information, because it creates and implements information security, but (unfortunately) on the distort (Tepšić, 2010).

EMPIRICAL PART

Scope and objectives of the research

In line with previous theoretical analysis, the subject of empirical research is the analysis of information security in organizations, with an emphasis on cyber security. The main problem is to establish how organizations assess, develop, create and support their programs to ensure information security.

Research tasks

In order to prove or disprove hypotheses, it is necessary to realize the tasks of the research. As a part of the work, it is needed: to examine the presence of cyber incidents, investigate the maturity of corporate information security in Serbia; prepare an overview of commonly used security measures; examine the awareness of organization’s information security; determine how control of third parties is present in the organization; determine if there is audit and testing principles of information security.

Research hypotheses

Based on the object and purpose of the research, hypotheses were defined:

H1 Majority of companies were not victims of cyber attacks.
H2 In most companies’ policies, procedures and spheres of responsibility in the field of information security were established.
H3 Presence of control of third parties is at a low level.
H4 Top management and end-users are not sufficiently aware of the risks of cyber security.
H5 Special protection systems are poorly represented.

Research methods

Qualitative and quantitative approach were combined, so-called triangulation method. The techniques and instruments were selected as part of the descriptive research method. Analytical- synthetic and statistical methods were also applied.

From research techniques in the process of collecting data, we applied: interviews, surveys and scaling.

The instrument we use is made from the questionnaire for determining the level of information security in organizations in Serbia, that has been created for this research.

The research sample

The sample consisted of managers of services for corporate security of 53 companies from Serbia, which are members of Serbian Association of Managers of Corporate Security. There was 43% of companies in the financial sector, 22% of trade, 14% consecutively of technology and telecommunications, and 7% of production. The sample is adapted to analytical needs of this research, and is deliberate.

The survey was conducted online during the period from May 5th 2016 to July 1st 2016.

The research results

We came to the results based on the analysis of questionnaires. The questionnaire was analyzed from five aspects:: the maturity of corporate information security; the most commonly used security measures; awareness of information security; presence of control of third parties; existence of audit and testing principles of information security.

The questionnaire contained 26 questions, according to the given aspects, which were analyzed and processed.

In Table 1, answers to the question of exposure to attacks over the last 12 monthswere given.

Based on the research results, we can conclude that our hypothesis H1 M*ajority of companies were not victims of cyber attacks*, was confirmed.

Table 1:Exposure to attack in the last 12 months

Have you been under attack in the last 12 months?	
Contention	%
No	65
Virus attacks	15
Hacker attacks	0
Harmful Software	8,6
Lost portable devices	0
Exploitation of vulnerabilities in the framework of test	3
I have no information	5
Something else	3,4

On the question of standards for managing IT, the majority of respondents replied that they possess internal policies - 65%, followed by regulatory requirements - 50%, but international standards such as COBIT or ITIL - 35%.

Some research questions related to the level of maturity of information security in relation to the following elements: 1. awareness of respondents about network security, 2. availability of policies, 3. the extent to which the responsibility for information security is specified, 4. current level of maturity and 5. key aspects of improving corporate information security.

64% of respondents believe that their organizations have adequate policies and procedures (question 5) providing security. Interestingly, there were no respondents who answered that their organization has none or weak policies and procedures. It is worth noting that the majority of organizations have policies and procedures in relation to: 1. IT security strategy and 2. plans of securing the continuity of business (question 6). A number of respondents said that their organizations worked out a plan to react to incidents in the area of cyber security (see Table 2).

Table 2: The organizational policies and procedures

Which of the following policies / procedures are documented and established in your organization (possibility of more than one answer)	
Contention	%
Strategy for information security	57
Ensure business continuity plan	57
Information Security Management Structure	35
Action Plan for Information Security	38
Does not exist, but working on it in the next 12 months	15
Response plan to the incidents in the area of cyber security	22
None of the proposed	15

Analysis of answers in the field of policies and procedures has shown that we can confirm our second hypothesis H2 In most companies'policies, procedures and spheres of responsibility in the field of information security were established.

Replies to question 7 show that 57% of organizations have an employee in the security sector, while the remaining 43% still don't have such a position in their systematization. Responsibility for information security is, as a rule, assigned to the head of the IT department or chief executive officer (CEO) - 36% of responses, or else to the board of directors - 14% (question 8).

Most of the organizations surveyed, about 80%, are informed about information security via professional publications or through certain specialized websites (questions 9 and 10). About 10% of organizations had a personal experience with attacks, or attacks with their clients, while 20% of them attend professional conferences and roundtables.

Given the fact that every organization has a different organizational structure and has to deal with various security threats, we assume that more of them will be ready to learn about this problem at seminars and conferences, as well as to engage the appropriate consultants.

The question 11 referred to the assessment of the current level of information security, based on our five-stage models. As shown in Table 3, about 30% of respondents believe that their organization is located on the 3rd level, which means that "there is a set of defined and documented standard processes, we can see some degree of improvement over time."

Table 3: The level of maturity of the organization

At what level of maturity is your organization today	
Contention	%
First, the basic: no documents, the dynamics will change depending on the situation, uncontrolled reacting to circumstances, success depends on the efforts of individuals.	15
Second, repeating: some processes are repeated with possible reliable results, the low level of discipline in processes, agreed standards.	15
Third, fixed: there is a set of defined and documented standard processes, we can see some degree of improvement over time.	30
Fourth, manageable: benchmarking processes, effective management control, adaptation without losing quality.	10
Fifth, optimized: the focus on continuous improvement and innovation	10
Can not estimate	20

To achieve maturity level 3, it is important that the policies and procedures are implemented throughout the organization.

At the end of this segment, we asked respondents to indicate what would raise the level of maturity of information security (question number 12, it was possible to select more than one argument). Most of them replied that it would be: 1. possession of more modern instruments - 60%, 2. higher level of informing - 70% and 3.readiness of top management to raise the level of information security - 55%.

The second segment of the study was devoted to aspects of the most commonly used measures.

Here is a review of information security threats perceived by respondents as the most dangerous in relation to their organization, and security measures that are applied to their control and prevention of the cyber attack.

The research results in this segment were very diverse, suggesting a wide range of cyber security risks faced by the organization in Serbia (question 13). The largest percentage of respondents, even 55%, considered hacker attacksto be the most dangerous, followed by 50% of those who identified uncontrolled portable devices, the same percentage is given toallegations of harmful software and insider attacks; threats from the Internet are following with about 40%, then viruses from e-mail with 35%, illegal software with 20% (note that it was possible to choose more claims).

Questions 14 i 15 indicatethat most organizations apply basic security measures - antivirus, firewalls and access control lists. However, modern solutions are used very few, such as intrusion prevention, file encryption, vulnerability management and control of system records, system events and operations research, due to the fact that hackers around the world are rapidly becoming more sophisticated in their hacking techniques.This indicates that the current state of security in Serbian companies can be the main threatto itself.

Question 16 showed that companies in Serbia mainly use commercial products for protection, not solutions specifically programmed for a specific company. It is important to note that, if you use a commercial products, periodic renewal of the license is mandatory in order to ensure adequate protection of the most widespread threats.

We believe that continuous investment in the studies of the security risks, and in the tools and techniques to ensure the system, can reduce the security risk to an acceptable level. This includes the development of measures that take into account the specificity of certain companies, ie. types of activities as well as information on intellectual property.

The third segment is about the awareness of information security.

As we could conclude on the base of questions 9 and 10, on the risks of cyber security IT departments learn mainly from trade journals.

Despite the fact that they are well informed about the risks of cyber security, end-users and top management are at a very low level of awareness. This we conclude on the the percentage of nearly 50% negative responses to question 17–Does your organization apply training for employees to raise awareness of information security?. Only 5% of companies in our research conduct such trainings according to the levels of access to information.

On the questions 18, 19 and 20, relating to financial investment in information security, the highest percentage of responses was that this information is not available - over 65%. It can be assumed that respondents consider this information confidential.

The fourth and fifth segment of the research is turned to the presence of control of third parties, or the existence of audit and testing principles of information security.

Analysis of the responses has led to the conclusion that control of third parties (suppliers and partners) is in accordance with safety standards, ie. it is insufficient. 50% of respondents believe that this control is determined by the signing of an agreement on the confidentiality of information, and 36% that it is determined by agreement. 50% of them believe that the control provides access through access policy, but only 15% have more stringent control measures such as spot checks, audits of third parties or formal third parties certification.

Audit and testing of information security is implemented only by 21% of organizations, 43% do not implement it, while 36% of respondents did not have information about it, which leads to the conclusion that it is not performed in these organizations, and that raises the percentage of organizations in which audit and testing are not implemented to 79%.

Analysis of answers relating to other segments of the survey confirmed our hypothesis: H3 presence controls of third parties is at a low level; H4 Top management and end-users are not sufficiently aware of the risks of cyber security; H5 Special protection systems are poorly represented.

Audit and testing provides important information to top management on the current state of maturity of information security in the organization. For effective protection, it is necessary to implement testing and audit with the professionals and in accordance to international standards. Regular testing and audit allow reducing the risk of cyber attacks.

CONCLUSION

Regardless of the fact that an increasing number of companies are paying attention to the corporate informational security, we can conclude that there is a high risk of leakage of confidential information.

To get to know the current state of information security program and management structure of the Serbian organizations, we conducted a survey on information security.

The research was focused on cyber security risks and for that purpose, 53 organizations, members of Serbian Association of Managers of corporate security, were tested.

After conducting the survey, five key conclusions about the current status of the program of corporate information security and cyber security in Serbian organizations singled out: 1. majority of surveyed organizations had not been exposed to cyber attacks;2. most organizations have established policies, procedures and spheres of responsibility for information security; 3. there is not enough control of third parties which is in accordance with safety standards ISO / IEC 27001: 2005, and ISO 27001; 4. top management, and end-users are not sufficiently aware of the risks of cyber security; 5. high level of protection measures is not applied, or applied to a very small extent.

It is important to note that the modern information security market is sufficiently developed to provide customers a wide range of solutions and services for the protection of each segment of information infrastructure. The most important thing is that the management, in cooperation with the IT sector, choose the right combination of protection components, consistent with business processes and information security policy, to establish an effective system of safety management of the company.

REFERENCES

[1] Global Data Leakage Report (2015). https://infowatch.com/report2015, dostupno 17. 8. 2016.

[2] http://www.infotech.org.rs/blog/wp content/uploads/KPMG-IT kontrole-i-upravljanje-rizicima-informacionih-sistema.pdf, dostupno 21. 8, 2016.

[3] Ivandić Vidović, D., Karlović, L., Ostojić, A. (2011). Korporativna sigurnost, Udruga hrvatskih menadžera sigurnosti – UHMS, Zagreb

[4] Kolaric, B. Arsenijevic, O. Radojcic, S. (2011). The organizational barriers in sharing knowledge and collective learninig: a case study of Telecom Serbia, International Tehnology, Education and Development Conference (IATED), INTED2011 Proceedings CD, www.iated.org

[5] National Information Systems Security Glossary (2000). NSTISSI No 4009, National Security Agency, Fort Meade MD

[6] Rodić, B., Đorđević, G. (2004). Da li ste sigurni da ste bezbedni, Produktivnost, Beograd

[7] Stojanović, T. Djokić, A. Djokić, S. (2013). Organizational Behavior-Creative Tool for Creating Value, International Review, No. 1-2.

[8] Tepsic, M. (2010). Some aspects of information security in the system of public administration in the Republic of Srpska, News, Journal of Social Issues. UDC 351.9 [005:004 (497.6RS), Banja Luka, Bosnia and Herzegovina

[9] The e-Crime Report (2011). Managing risk in a changing business and technology environment, (2011).

[10] Trivan, D. (2012). Korporativna bezbednost, Dosije studio, Beograd

[11] Информационная безопасность бизнеса, (2014). http://www.kaspersky.ru/images/Bezopasnost_Screen.pdf, dostupno15. 8. 2016.

[12] Результаты исследования информационной безопасности в Центральной Азии, (2014). http://www2.deloitte.com/kz/ru/pages/risk/articles/risk-ca-security-survey-2014.html, dostupno 19. 8. 2016.

Article history:

- **Received 29 September 2016**
- **Accepted November 2016**