SECURITY OF INFORMATION ASSETS IN SMALL AND MEDIUM-SIZED ENTERPRISES

FRANTIŠEK KORČEK[1] – VLADIMÍR BOLEK[2] – MARTINA BEŇOVÁ[3]

Bezpečnosť informačných aktív v malých a stredne veľkých podnikoch

***Abstract**: The period of information and communication technology development is associated with increased information security risks. The risks affect information assets of small and medium-sized enterprises, which are vulnerable due to rapid development and the lack of available financial resources. The priority of SME is to improve the security level in ICT, as the price for the loss of confidential data and business secrets is too high, in some cases even existential. Therefore, it is essential to examine and assess the security of information assets as the part of information security risk management in SME. The paper contains results of the research that evaluates the importance of individual information assets in Slovak enterprises and presents the usage of technical and organisational measures protecting the assets.*

***Keywords**: information security, information assets, small and medium-sized enterprises, risk management, security measures*

JEL Classification: M 15

1 Introduction

Information and communication technology (ICT) has become an essential part of enterprises. A large number of enterprises is completely dependent on ICT and cannot perform their business activities and compete with the competition without ICT. It coincides with many business processes and provides benefits to entrepre-

1 Ing. František Korček, Ekonomická univerzita v Bratislave**,** Katedra informačného manažmentu, Fakulta podnikového manažmentu, Dolnozemská cesta 1/B**,** 852 35, Bratislava, e-mail: frantisek.korcek@euba.sk

2 Ing. Vladimír Bolek, PhD., Ekonomická univerzita v Bratislave**,** Katedra informačného manažmentu, Fakulta podnikového manažmentu, Dolnozemská cesta 1/B**,** 852 35, Bratislava., e-mail: vladimir.bolek@euba.sk

3 Ing. Martina Beňová, Ekonomická univerzita v Bratislave**,** Katedra manažmentu, Fakulta podnikového manažmentu, Dolnozemská cesta 1/B**,** 852 35, Bratislava., e-mail: martina.benova@euba.sk

The research described in the paper was financially supported by the Project of Young Researchers and Full-time PhD Students at the University of Economics in Bratislava, no. I-15-103-00.

neurs in the form of electronic communication, processing of business data, specialised software, cloud storage, etc. However, it becomes a source of exposure to information risks that affect business information assets. Loss, damage, theft or total destruction of replaceable or irreplaceable assets leads to damages that many enterprises might not overcome. For this reason, it is important for businesses to direct a part of their income to the protection of their core information assets.

The issue of information asset security is targeted on Slovak small and medium-sized enterprises (SME, number of employees from 10 to 250), which are becoming increasingly threatened by security incidents, but lack comprehensive education in information security controls or their progress is rather slow. Many of the Slovak SMEs do not possess sufficient financial resources [12] to purchase advanced tools of information security tools and staff training, respectively, to have enough time and high quality personnel to develop organisational measures. Nevertheless, SMEs administer a crucial role in the economic system of a country. They provide employment for the majority of the workforce and are more dynamic and more innovative than large companies.

This research paper provides a summary of the sectional results of a project for researchers and full-time PhD students at the University of Economics in Bratislava, "Information security risk management in small and medium-sized enterprises, no.I-15-103-00." The project aims at analysing the current information security issues and the risk management in SME arising from the information security events.

2 Information Security Risk Management

Security of information assets belongs to information security risk management (ISRM), which is further specified in the standard of ISO/IEC 27005. The standard provides guidance on the implementation of risk management in order to meet the requirements for the information security management system (ISMS) described in ISO/IEC 27001 [13]. This family of standards defines ISRM as a continuous process that determines the context, assesses and treats the risks, implements the recommendations and decisions [14].As a business process, ISRM is logically and sequentially arranged set of activities having a common objective, where the output from the previous activity is connected with the input of the next activity [2].

If enterprises want to increase the security level of their information assets, they need to address the process of risk management, which includes a variety of activities such as setting the context, identification and assessment of the assets, risk analysis and evaluation and a risk management plan [10]. Introduction of the risk management process in the issue of information security has the following reasons for the organisation: ensuring the market and efforts to protect information assets, thus demonstrate that confidentiality, integrity and availability of information maintains at all times [9].

According to a global survey conducted by Ernst & Young, 53% of organisations claim that one of the main causes of difficulty in information security is a lack

of experienced and capable resources [5]. At the same time, the results of a survey conducted by Kaspersky Lab show that 90% of enterprises admitted security incident and 46% of enterprises lost sensitive data due to an internal or external threat. On average, enterprises pay up to $620000 to recover from a security breach and small businesses spend $46000 [8]. Such amounts might lead many enterprises into existential crisis. The financial losses caused by security breaches usually cannot be precisely detected in enterprises, because a significant number of losses come from smaller-scale security incidents causing an underestimation of information system security risk [6]. Thus, managers need to know threats that influence their assets and identify their impact to determine what they need to do to prevent attacks by selecting appropriate countermeasures [7]. Similar data was acquired by PwC organisation, which identified 90% of large and 74% of small enterprises having a security breach this year [11]. These global statistics confirm that a systematic protection of information assets is a necessity.

Businesses are aware of the difficulties caused by the information risks, but do not take the necessary steps to enhance their information security. In the period of swift availability of good quality information, ignorance is an inadequate justification. SME need to apply the available models, techniques and staff trainings to implement the adequate ISRM. Adequate security is a level of security that achieves the smallest impact of risks at an acceptable cost of their measures [4].

2.1 Security of Information Assets

Information assets are defined as everything that has a value for the enterprise. The simplest division is into tangible and intangible assets. There are many types of assets including information, software, physical assets (e.g. a personal computer), services, personnel, its skills and experience, intangible assets (e.g. know-how, reputation) [13, 4, 3]. Majority of authors rank among the assets with a high value customer data, financial statements, financial systems, marketing strategies, various personal data, research and development data, sales information and source codes[1]. Managers must first identify and quantify their information assets, then proceed to security. Protecting information assets is an important activity in relation to all stakeholders such as business partners, employees, customers, suppliers and others [12].

Security of information assets is performed by using a variety of technological and organisational measures. Information security measures involve various methods (e.g. physical, procedural, hardware, software, and personnel methods) that are employed to detect, prevent or minimise losses associated with the threats to an information system [15, 16]. It is significant to obtain measures at reasonable costs while providing adequate protection from security incidents. Majority of Slovak SMEs use only basic or inexpensive tools including antivirus programs, regular software updates, elementary settings of Wi-Fi networks, uninterruptible power supplies, security alarms and camera systems, etc. More advanced tools and organisational measures (e.g. policy of strong passwords, backup plans) seem to be

inaccessible to SMEs as they do not often possess sufficient financial and personnel resources.

3 Objectives and Methodology

The main scientific objective of the research paper is to evaluate the significance of individual information assets and to discover the most important assets to Slovak small and medium-sized enterprises. It reflects the current state of knowledge of the issue. The main objective is supported by following sectional objectives:

- To evaluate the percentages of total costs spent by SMEs to secure information assets,
- To examine the satisfaction of SMEs considering their current security level,
- To assess the usage of security countermeasures in order to search for the most common measures applied in SME.

Several scientific methods are used to meet the objectives of the paper. Firstly, domestic and foreign scientific literature is compared to analyse the basis of the issue. Subsequently, a survey consisting of a structured questionnaire distributed via internet targets Slovak small and medium-sized enterprises. The questionnaire was designed by justifying valid content, construct and criteria. Later on, reliability and accuracy is determined by the frequency of items, homogeneity and complexity of the tasks. The collected sample of 83 respondents segmented into selected groups and expressed in percentages is presented in the chapter of results.

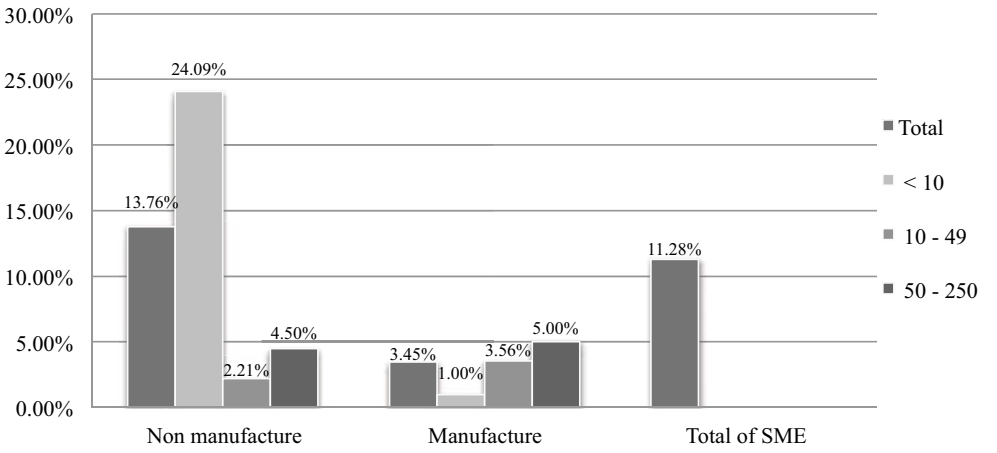
Methods of descriptive statistics and the application of qualitative and quantitative statistical methods are used to analyse the survey sections. Conclusions of the research are formulated by using methods of comparison, deductive reasoning,general analysis and synthesis. The practical knowledge and theoretical assumptions are combined in order to achieve results of the sectional issue areas.

4 Results

The survey revealed that in average, SME use 11.28 % (M = 11.28 %, SD = 18.44 %) of their total costs on the protection of information assets against unwanted security incidents. Minimum value stated by respondents is 1 % and maximum value corresponds to 60 %. Three quarters of surveyed enterprises spend up to 10 % of total costs to protect the assets. Half of businesses dedicate up to 5 % of total costs to improve their information security level. The average value of around 11 % of total costs would have been ideal for business information security, if the majority of studied enterprises had not invested less in security assets. The average percentages of total costs spent on security of information assets are shown in Figure 1. Data is segmented by the type of business into manufacturing and non-manufacturing businesses. Within such division, data is further segmented by the number of employees to distinguish between the sizes of enterprises.

Figure 1

Average percentages of total costs spent on the security of information assets



Source: authors' calculations.

Notes: Data is segmented by the type of business and the number of employees. Non-manufacturing enterprises employ 13.76 % of the costs to secure their information assets, while manufacturing enterprises only 3.45 % on average. This is affected by non-manufacturing enterprises that are primarily engaged in providing services, where most business processes and operations are automated by ICT. These technologies are logically more vulnerable to information threats. Businesses providing services realise this fact, therefore invest more in information security than manufacturing enterprises.

On average, non-manufacturing microenterprises (less than 10 employees) invest in information security the most, 24.09 % of total costs. Non-manufacturing medium enterprises (up to 250 employees) use 4.50 % on average, which seems too low, but those enterprises have several times higher costs than small or microenterprises. Therefore, 4.50 % of total costs represents a relatively large amount. On a similar level, manufacturing medium-sized enterprises spend 5.00 % of total business costs. Leaks of confidential information or loss of sensitive data for a medium enterprise have greater consequences than for a small business.

Results of another section of the research are shown in Table 1, which demonstrates the evaluation of SME satisfaction with their security level of sensitive information (personal data, business secrets, confidential data). On a scale from 0 (not satisfied at all) to 7 points (very satisfied) managers rated their current feeling whether their information security is sufficient. The mean score is equal to 4,49p, SD = 2,12p, which is more than the average of the rating scale. More than a half of enterprises selected a value 5 and more. Generally, SME are satisfied with their level of information security, which is also confirmed by a value 6 selected by 31.3 % of

SMEs and a score 7 selected by 10.8 %. No enterprise picked value 1. Only 12.0 % of SMEs are not satisfied with their security level at all.

Table 1

Satisfaction of SME considering their security level of sensitive information

Number of employees in the enterprise		*Rating scale of satisfaction*							*Total*
		0 (MIN)	*2*	*3*	*4*	*5*	*6*	*7 (MAX)*	
< 10	*%*	9.6%	6.0%	7.2%	0.0%	9.6%	8.4%	1.2%	42.2%
10 - 49	*%*	2.4%	0.0%	0.0%	9.6%	12.0%	10.8%	7.2%	42.2%
50 - 250	*%*	0.0%	0.0%	0.0%	1.2%	0.0%	12.0%	2.4%	15.7%
Total	*%*	12.0%	6.0%	7.2%	10.8%	21.7%	31.3%	10.8%	100.0%

Source: authors' calculations.

When analysing the satisfaction of researched enterprises segmented by the number of employees, we noticed that medium-sized businesses selected only values 4, 6 and 7. Their satisfaction with the security of sensitive information is high. The satisfaction of small enterprises (10 – 49 employees) is above the average as well. Only 2.40 % of these businesses is not satisfied with the level of security at all. Even if the small enterprises' contentment in the level of security is above the average, the costs spent to secure information constitute only 2.21 % of total costs for non-manufacturing and 3.56 % for manufacturing enterprises. This means that either they use organisational and technological measures at the actual costs at a good level, or such businesses do not recognise adequate information security, or they underestimate threats of security incidents.

4.1 Significance of Information Assets

Subsequently, we examined the significance of information assets for SME in the survey. On a scale from 0 (easily replaceable) to 7 points (irreplaceable) respondents determined the importance of information assets for their business processes and operations, as well as the impact of the loss or theft of individual assets. Table 2 reports the results and is sorted by the most significant information assets.

Table 2

Significance of information assets to small and medium-sized enterprises

Nº	*Information asset*	*N*	*Min*	*Max*	*Mean*	*Std. Deviation*
1	*PC, notebook*	83	1,00	7,00	6,1325	1,53632

N°	*Information asset*	*N*	*Min*	*Max*	*Mean*	*Std. Deviation*
2	*Backup and archive data*	83	1,00	7,00	5,8434	2,06883
3	*Server*	83	,00	7,00	5,7470	2,16312
4	*Data from the information system*	83	1,00	7,00	5,7108	1,61947
5	*Internet connection*	83	1,00	7,00	5,6867	2,15796
6	*Contracts and relationships with business partners*	83	2,00	7,00	5,6506	1,92818
7	*Knowledge of employees*	83	1,00	7,00	5,6386	1,30270
8	*Accounting data*	83	2,00	7,00	5,6145	1,81344
9	*Availability of e-mail service*	83	,00	7,00	5,6145	2,20217
10	*Business secret and know-how*	83	1,00	7,00	5,4337	2,17633
11	*Active components of computer network*	83	1,00	7,00	5,1566	1,80434
12	*Database*	83	1,00	7,00	5,0602	2,13764
13	*Operating system of a computer*	83	,00	7,00	4,9518	2,11789
14	*Personal data*	83	,00	7,00	4,8554	2,31713
15	*Operating system of a server*	83	1,00	7,00	4,8434	2,23869
16	*Hardware devices (scanner, printer,...)*	83	1,00	7,00	4,7349	2,27973
17	*Office software*	83	,00	7,00	4,4940	2,26518
18	*Web page*	83	,00	7,00	4,4578	2,52452
19	*Database system*	83	,00	7,00	4,3855	2,54631
20	*Workplace network connection*	83	,00	7,00	4,1325	2,92079

N°	*Information asset*	*N*	*Min*	*Max*	*Mean*	*Std. Deviation*
21	*Security system (CCTV, UPS, alarms...)*	83	,00	7,00	4,0241	2,34248
22	*ERP system (business management software)*	83	,00	7,00	3,7711	3,05369
23	*Specialised software*	83	,00	7,00	3,5422	2,74662
Valid N (listwise)		83				

Source: authors' calculations.

In the conducted survey, enterprises identified personal computers as the most significant information asset (M = 6,13p, SD = 1,54p). This information is a bit misleading, because although businesses correctly determined that PCsare important, but probably perceived PCs as the significant data contained in their computers. If PCs were seen asa hardware or as a device, they would reach a different position in the table. The argument is proven by a second row in the table, backup and archive data (M = 5,84p, SD = 2,07p). Along with a server (M = 5,75p, SD = 2,16p) and data from the information system (M = 5,71p, SD = 1,62p), the backup data is the most important information asset in Slovak SME. Internet connection is the fifth significant asset (M = 5,69p, SD = 2,16p) for SME. Nowadays, working with the Internet is obvious and irreplaceable. In theory, this asset might not gain a higher position as business data will be of increasing significance.

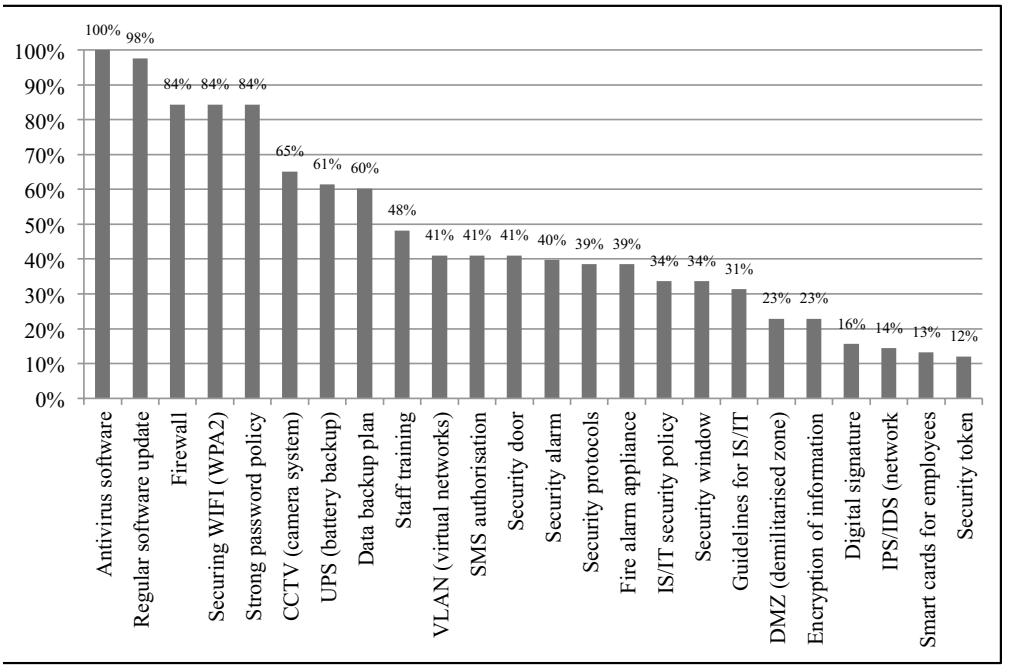
In the first half, up to four points on the scale, only two information assets are placed – ERP system (M = 3,77p, SD = 3,05p) and specialized software (M = 3,54p, SD = 2,75p) that are considered less significant, resp.replaceable. All the other information assets are rated by four or more points on average, thus perceived as significant. An interesting result is the evaluation of personal data (M = 4,86p, SD = 2,32p), which we expected to get a much better appreciation, because its disclosure or theft might lead to existential problems of the enterprise. Therefore, the researched sample of SMEs presumably does not pay enough attention to personal data.

4.2 Security Measures

Small and medium-sized enterprises secure their information assets by various measures, tools, procedures and metrics. In Figure 2, a sorted percentage overview of the different organisational and technological measures, which are used by SMEs, is shown. Studied enterprises could choose from several options, depending on which measures they actually apply in their own processes of information security management.

Figure 2

Percentage of SME using selected security measures



Source: authors' calculations.

The results confirm that all respondents use antivirus software against malware. Many businesses are limited by perceiving antivirus softwareas the only sufficient measure to eliminate all threats of information security. From our point of view, the crucial countermeasure of information security is a staff training, which is unfortunately located in the ninth position with 48% usage in enterprises.

Many security incidents may be eliminated by organisational measures at low costs. Such measures are the staff training, guidelines for IS/IT operation by employees (31 %), a document of IS/IT security policy (34 %), which is used by more than a third of SME only, and a policy of strong passwords (84 %). Only the password policy is applied in enterprises quite often. In the survey, we expected better results from the selection of effective security tools such as demilitarised zone (23 %) used in a network, software for encryption of information (23 %), digital signature (16 %), intrusion prevention and detection systems (14 %) that monitor networks and identify security breaches, and smart cards for employees (13 %). These techniques might be expensive for SME. The survey results confirm that SME do not own available and sufficient funds to protect their irreplaceable information assets. Moreover, the research reveals that enterprises at least secure their information assets by basic technological or organisational measures.

5 Conclusions

To conclude, security of information assets is progressively being integrated into the business activities of SME along with the development of ICT. Due to the increase in the number of security incidents and in expenses to remedy information security breaches, SME are beginning to realise the potential threats and consequences. The ideal solution is to introduce the process of active information security risk management.

The impact of security incidents on tangible and intangible information assets in SME is compensated by using part of total costs on information security issue. 75 % of surveyed businesses spend up to 10 % of total costs. Microenterprises aimed at service providing protect their assets by investing 24.09 % of their total costs. At the same time, managers of such enterprises reported a low score of satisfaction with the level of information security. Unlike microenterprises, small and medium-sized enterprises invest less on the average (up to 5 % of total costs), but their satisfaction with the security of assets is considered positively.

SMEs include personal computers, backup and archive data, server, data from the information system and internet connection into a group of irreplaceable information assets. Data is still the most important asset because it contains sensitive information of businesses. Internet connection becomes a necessity, as many SME cannot run their business operations without it. We expected the assets of personal data, business secret and know-how to be more significant. Supposedly, the respondents do not possess such assets or simply do not work with the assets on a daily basis.

The most commonly used and also essential measures for securing information assets in the enterprises are the antivirus software and regular software updates. Other measures that are often used include firewalls, WPA2 and the policy of strong passwords. Organisational measures (staff training, IS/IT security policy and guidelines for IS/IT operation) reached only average percentages. Effective tools such as DMZ, encryption of information, digital signature, IPS/IDS and smart cards are almost not applied. We assume that the reason is their price as well as scarcity of skilled human resources to acquire and operate the tools in examined enterprises. Therefore, SME need to elevate the level of employees´ education in the field of information security and spend more efforts and financial resources on risk management. We recommend to reconsider the importance of individual information assets by managers of SMEs as their value is different in each enterprise. Subsequently, it is crucial to select countermeasures that provide an adequate level of information security at acceptable costs. The main scientific objective and the sectional objectives of the paper are met by evaluation of the significance of individual information assets, the usage of security measures, the SME satisfaction with their level of information security and the proportions of the total costs spend by researched SME for the security of information assets.

References

[1] ANONYMOUS: *Maximální bezpečnost*. (Maximum security). Praha: Softpress, 2004. ISBN 80-86497-65-8.

[2] BODIŠ, M.: *Procesné riadenie vo väzbe na infraštruktúru podnikových informačných technológií.* (Process management related to enterprise information technology infrastructure). Bratislava: Ekonóm, 2014. ISBN 978-80-225-3984-5.

[3] ČERMÁK, M.: Řízení *informačních rizik v praxi.* (Managing information risks in practice). Brno: Tribun EU, 2009. ISBN 978-80-7399-731-1.

[4] DOUCEK, P.: Řízení *bezpečnosti informací.* (Management of information security). Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

[5] ERNST & YOUNG: *Get Ahead of Cybercrime: EY's Global Information Security Survey – 2014.*Available athttp://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf

[6] GERIC, S. – HUTINSKI, Z.: Information system security threats classifications. In: *Journal of Information and Organizational Sciences.* Vol. 31, Issue 1, pp. 51-61. ISSN 1846-9418.

[7] JOUINI, M. – RABAI, L. B. A. – AISSA, A. B.: Classification of Security Threats in Information Systems. In: *The Fifth International Conference on Ambient Systems, Networks and Technologies (ANT-2014).* Hasselt, Belgium: Hasselt University, pp. 489-496.

[8] KASPERSKY LAB: *Damage control: The cost of security breaches, IT security risks special report series.* Available at: http://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf.

[9] MAKATÚRA, I.: *Riadenie bezpečnosti informácií podľa nových noriem.* (Information security management according to new standards). Available at: http://www.itnews.sk/2014-04-24/c162824-riadenie-bezpecnosti-informacii-podla-novych-noriem/.

[10] ONDRÁK, V. – SEDLÁK, P. – MAZÁLEK, V.: *Problematika ISMS v manažerské informatice.* (ISMS problems in managerial information science). Brno: CERM, 2013. ISBN 978-80-7204-872-4.

[11] PWC. *2015 Information Security Breaches Survey: Executive Summary.* Available at: athttp://www.pwc.co.uk/assets/pdf/2015-isbs-executive-summary-digital.pdf, [accessed 17. 10. 2015].

[12] STEHLÍKOVÁ, B. – HOROVČÁK, P. : *Manažment informačnej bezpečnosti v malých a stredných podnikoch.* (Information security management in small and medium-sized enterprises). Available at: http://www.securityrevue.com/article/2012/06/manazment-informacnej-bezpecnosti-v-malych-a-strednych-podnikoch.

[13] STN ISO/IEC 27000. *Information technology. Security techniques. Information security management systems. Overview and vocabulary.* Bratislava: Slovak office of standards metrology and testing, 2014.

[14] STN ISO/IEC 27005. *Information technology. Security techniques. Information security risk management. Requirements.* Bratislava: Slovak office of standards metrology and testing, 2012.

[15] TSIAKIS, T.: Consumers' issues and concerns of perceived risk of information security in online framework. The marketing strategies. In: *World Conference on Business, Economics and Management.* Antalya, Turkey, pp. 1265-1270.

[16] ZHANG, J. – REITHEL, B. J. – LI, H.: Impact of perceived technical protection on security behaviors. In: *Information Management and Computer Security.* Vol. 17, Issue 4, pp. 330-340. ISSN 0968-5227.