PRACTICING INFORMATION SECURITY MANAGEMENT SYSTEM IN E–COMMERCE

[a]FRANTIŠEK KORČEK, [b]VLADIMÍR BOLEK, [c]ANITA ROMANOVÁ, [d]PATRIK RICHNÁK

University of Economics in Bratislava, Faculty of Business Management, Dolnozemská cesta 1, 852 35 Bratislava, Slovak Republic
email: [a]frantisek.korcek@euba.sk, [b]vladimir.bolek@euba.sk, [c]anita.romanova@euba.sk, [d]patrik.richnak@euba.sk

The research described in the paper was financially supported by the Slovak Grant Agency (VEGA) under grant No. 1/0436/17 and the Project of Young Teachers, Researchers and Full-time PhD. Students at University of Economics in Bratislava, No. I-18-102-00 Implementation of modern concepts in business logistics in Slovakia in the era of digital technology

Abstract: Doing business through e–commerce is now a common way of selling goods and services for any types of business organisation. However, many entrepreneurs do not sufficiently secure their e–business processes due to being unaware of the seriousness of threats that affect business information assets in cyberspace. Information security management system is not widely used in e–commerce businesses, thus leaving processes vulnerable against information security risks. This paper examines differences in the use of the system between e–commerce businesses that assess or do not assess the information security risks and verifies the effect of practicing this system on the information security level in the e–commerce businesses.

Keywords: information security, e–commerce, information security management system, information assets, risks

1 Introduction

From a global point of view, there is a constant increase in the entry of enterprises with various business subjects into the electronic market of goods and services. The reasons are clear: multiple market expansion, improved competitiveness and marketing, increased brand awareness of potential customers, an increase in orders and the associated increase in sales, etc. A country which recorded the most electronic sales of approximately 838 120 million € in 2016 is China. Followed by the United States (331 890 million €), the United Kingdom (139 120 million €) and Japan with a total turnover of 103 920 million € (Keith, 2015). In 2016, the total turnover from sales through online stores in Slovakia amounted to 900 million € (Dvorský, 2016), the Czech Republic reached 3 760 million € (APEK, 2017). Compared to the world leaders, the amounts are low, but the numbers are affected by the size of the country's population. E–commerce purchases are mostly made by UK citizens (2 140 € per inhabitant per year), the US citizens (1 024 €) and Japanese (824 €). In Slovakia, the population annually spends 166 € through e–shops, whereas the Czech citizens spend 356 €.

Many start–ups and well–established enterprises are not aware of the fact that doing business in the electronic marketplace, which is part of the cyber space, always brings new, but different threats than the threats in the ordinary course of business. In unprepared enterprises, information security threats can easily be implemented in the form of security incidents. Such enterprises have little knowledge of the threats, security incidents, and lack advanced capabilities to secure their information assets, notably due to the unidentified need to address information security issues by the business management, but also due to a lack of financial and material resources, unskilled and inexperienced employees. These shortcomings are common in e–commerce enterprises. The offer of goods and services to customers on the internet, i.e. the introduction and active use of e–commerce, is undoubtedly a modern way of offering products. Securing internal or external threats, environments, devices, business processes, business secrets, supplier and customer relationships might be obsolete in today's businesses due to the continued and rapid development of ICT. Therefore, it is necessary to review and evaluate the current state of information security management in enterprises that conduct business activities in the electronic market.

2 Literature review

2.1 Information security management system

Information is an asset that must be properly protected in a growing and interconnected business environment (Said et al., 2013). Information security is a highly popular topic for enterprises as they process and classify a lot of information on daily basis, many of which is considered confidential. The enterprises want this information to be kept secret from uninterested persons for various reasons, because its loss, disclosure or loss can lead to a business crisis. Information security needs to be managed, ideally by creating the information security management system (ISMS).

Information is a crucial part of every enterprise. Acquisition, processing, storage and secrecy of information are among the most important activities of the enterprise's life (Kokles and Korček, 2015). To carry out such activities, it is necessary to take care of technical devices that serve to access information, to set up a system for handling the information carriers and to adhere to organizational principles for protection against damage. Information security is needed in relation to each interested party, such as customers, employees, business partners, suppliers, etc. Security deficiencies result from insufficient appreciation of the importance of information security management (Stehlíková and Horovčák, 2012). Within the development of ICT and competition, the protection of confidential information needs to be increasingly important because the ICT has become an instrument or subject of cybercrime (Kokles and Romanová, 2014). In the current highly globalized environment, it is imperative that businesses deal with the quality of products and services provided, as competition is not only for the domestic market but also for the world market. This is the reason why the company seeks to create a competitive advantage over other producers and service providers. Focusing on achieving high quality information means ensuring competitiveness over the long-term and stable, as the quality of the products and services as opposed to the price is immeasurable over time (Klátiková and Gubová, 2015).

By applying the system approach, it is possible to protect business assets against information security threats. ISMS deals with the issue in detail. Below are definitions from a variety of sources:

- STN ISO/IEC 27001 (2014) defines information security management as a system that "protects confidentiality, availability and integrity of information by introducing a risk management process and providing confidence to stakeholders that the risks are well managed",
- ESET (2014) considers ISMS to be the basis for managing security risks in order to establish, implement, operate, monitor, revise, maintain and improve information security in an organization,
- According to ENISA, information security management is a system that allows us to achieve the required qualitative characteristics of services offered by organizations, such as service availability, confidentiality and data integrity, etc. (ENISA a, 2015),
- Singh et al (2013) claim that ISMS is a system of balanced intersection of technical, managerial and human aspects of information security in an organization,
- Ondrák et al (2013) perceives ISMS as the effective and documented information asset management system that aims to eliminate their possible loss or damage.

According to the above definitions, we claim that ISMS is a comprehensive system that protects information from risks within the overall management system of an organization. At the same time, the information security management is not only about the introduction of technical measures, but especially

about the management, which is confirmed by ENISA (ENISA b, 2015). ISMS brings business continuity, competitiveness, profitability, prestige, elimination of threats and losses from realized risks.

2.2 Information security in e–commerce

In a typical e–commerce system where a customer visits websites, browses the product catalog and makes purchases, there are four main participants. The first is a customer who searches for a specific website via an internet browser. The website is usually run by a trader whose goal is to sell goods or services with a profit. Because the trader does not specialize in software development, he or she purchases the website from the provider. An attacker is the only illegitimate participant to whom exploitation of others brings benefits (Lokhande and Meshram, 2013). Using a variety of methods and techniques, the attacker attacks the customer, trader, communication, web server, network elements, and IT infrastructure of the provider. From another point of view, there are three vulnerable e–commerce points where security threats aim, such as the client, the server, and the mutual communication (Mohammadpourzarandi and Tamini, 2013). Laudon and Traver (2014) consider malware, potentially unwanted programs, phishing, unauthorized intrusion into the system, spam, identity theft, DoS and DDoS attacks, poorly secured server, client software, social networking problems, mobile devices and the cloud as the most common and the most harmful threats in e–commerce environments. We complete the list by other social engineering methods (e.g. pharming), remote computer spying, eavesdropping (e.g. man–in–the–middle attack), password attacks (guessing, resetting, capturing, rainbow tables, etc.), poor authentication, faulty security configuration of network devices, servers, clients and protocols, abuse of web application vulnerabilities, especially input validation (e.g. cache overflow, cross–site scripting, SQL injection) and many others (Lokhande and Meshram, 2013; PCI SSC, 2013). The success of electronic sales besides the uniqueness of a product, adequate price, a suitable system, the correct target group and marketing activities, largely depends on the ability to address threats by implementing appropriate security controls. The level of information security and the protection of business information assets is essential for an internet customer who is willing to provide personal data to the e–commerce and then buy products and services.

The use of the internet is growing rapidly every year, the availability of cheap mobile devices and the expansion of the internet have become key factors (Yazdanifard, Edres and Seyedi, 2011). E–business is developing directly in line with the expansion of the internet. Wherever the internet is available, new electronic markets are emerging. However, such development will not be possible unless enterprises adhere to basic dimensions of information security, or create a safe environment for their information assets. The main reason for possible bankruptcy is a customer because he or she is vulnerable to security incidents that are directed to e–commerce (Smith, Nah and Cheng, 2016). Any untreated and executed risk (e.g. leakage of login data) leads to immediate loss of reputation (Li, 2015), loss of the number of customers and thus to the existence of problems. At the current period of a large number of security threats, offensive methods and techniques, enterprises cannot afford to ignore information security. We claim that the right way for enterprises is to apply a procedural approach to ISMS that guarantees adequate information security for e–business by minimizing the consequences of risks by appropriate security measures at acceptable costs.

ISMS of e–commerce is a significant system that determines the health and sustainable development of an enterprise (Ji and Zou, 2016). Increasing cybercrime and its simplifying and availability to incompetent ICT users actively attack the information assets of enterprises with e–commerce systems, but from another point of view the enterprises are forced to apply proactive or reactive technical and organizational measures that ultimately lead to the implementation of ISMS. Based on the available knowledge, we agree with Netolická's (2012) and Král's (2011) statement that enterprises trading on the Slovak electronic market lack a comprehensive information security management system. In the paper we examine whether the statement is correct and corresponds to the real situation.

3 Research objectives and methodology

The main objective of the paper is to review and evaluate the implementation of ISMS in e–commerce enterprises and its impact on the perception of the level of information security in the enterprises surveyed. In order to achieve the stated objective, we formulate the following hypothesis:

- H_0: The impact of the ISMS practice in an e–commerce enterprise on the enterprise's specified level of information security is not statistically significant,
- H_1: The impact of the ISMS practice in an e–commerce enterprise on the enterprise's specified level of information security is statistically significant.

The partial objective is to compare differences in the ISMS practice among enterprises that assess information risks and which do not assess such risks. The differences of groups are tested for statistical significance. The objectives of the paper are achieved using statistical methods and general methods of scientific work. When examining the structure of a data set, we used descriptive statistics and the Kolmogorov–Smirnov test (K–S test) to verify normal distribution of the data. When examining relations between variables in the case of normal distribution, an independent samples t–test was used (Hanák, 2016) and, in the case of other distributions, a nonparametric Mann–Whitney U test. The hypothesis was verified by linear regression.

The data were collected in the form of an electronic questionnaire in enterprises trading on the Slovak electronic market. The number of respondents was 91, which we consider to be a representative sample with respect to data sensitivity and the number of e–commerce enterprises that reached 9355 in 2015 with a year–on–year increase of 1105 (Heureka, 2015). The following table lists variables whose values enter the data analysis according to the set objectives.

Tab. 1 Research variables

ISMS. Information security management system	
ISMS1	The need for the information security management system in the respondent's e–business
ISMS2	Practicing the information security management system in the enterprise
ISMS3	Regularity of information security risk assessment
ISMS4	The level of information security specified in the enterprise

Source: Authors' own research

All continuous questionnaire variables (ISMS1, ISMS2, ISMS4) were measured on a scale of 0 to 100 points, where 0 points are the minimum and 100 points are the maximum. ISMS3 is a categorical variable measured on the ordinal scale. The following table shows a structure of the data set by main customers and business size.

Tab. 2 The dataset structure by main customers and business size

Main customers	Business size			∑
	Microenterprises	SMEs	Large enterprises	
B2C	68,13 %	18,68 %	2,20 %	89,01 %
B2B	5,49 %	4,40 %	1,10 %	10,99 %
∑	73,63 %	23,08 %	3,30 %	100,00%

Source: Authors' own research

Up to 89,01 % of e–commerce enterprises provide goods and services primarily to individuals (B2C), of which 68,13 % are microenterprises, 18,68 % are SMEs and 2,20 % are large enterprises. 10,99 % of enterprises surveyed are focused on B2B,

of which 5,49 % are microenterprises, 4,40 % are SMEs and 1,10 % are large enterprises. Other e–commerce models like B2G were not checked by respondents in the survey.

4 Results

The results of the data analysis are examined in order to determine the current state of ISMS in e–commerce enterprises. The descriptive statistics of the variables, except for the categorical variable (ISMS3), are listed in Table 3.

Tab. 3 Descriptive statistics of ISMS1, ISMS2 and ISMS4

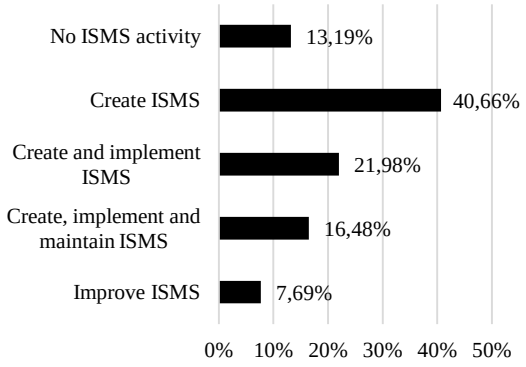
	N	Min	Max	Kurtosis	Skewness	Mode	Median	M	SD
ISMS1	91	1	100	-0,74	-0,41	100	60	61,26	29,33
ISMS2	91	0	100	-0,70	0,66	0	24	30,08	28,59
ISMS4	91	1	100	-0,68	-0,52	80	70	62,93	27,68

Source: Authors' own research

The ISMS1 variable measures the need to create, implement, maintain and continually improve ISMS in an e–commerce enterprise. We defined the scale from 0 (definitely not) to 100 points (certainly yes). 50 % of respondents rated this need for more or less than 60 points. The most frequently mentioned value was 100 points (15,38 % of respondents). On average, survey participants inclined to the need to improve the ISMS in their enterprise (M = 61,26; SD = 29,33). 75 % of respondents reported more than 46,5 points. The data are predominantly flat (-0,74) and right sloping (-0,41). According to the results of the K–S test at the significance level $\alpha = 0,05$, the data are normally distributed (Z = 0,89; p = 0,407). Therefore, we claim that the mean distribution value is between 55,16 and 67,37 points with 95% confidence.

ISMS2 follows in the survey and the variable examines whether enterprises are creating, implementing, maintaining, and improving the ISMS in their environment. The variable is specific because we categorized the values into four intervals that the respondents were familiar with. The values were divided into categories from 0 to 25 % (enterprises create ISMS), up to 50% (create and implement ISMS), up to 75 % (create, implement and maintain ISMS) and up to 100 % (improve ISMS). 0 % means that the enterprises do not perform any ISMS activity. Figure 1 shows the shares in the given categories.

Fig. 1 Share of enterprises practicing the ISMS

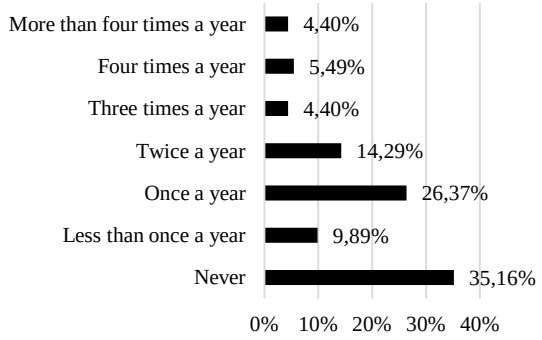


Source: Authors' own research

Most enterprises only create the information security management system (40,66 %), which is only in the initial phase. However, up to 13,19 % of enterprises do not operate in this area. Interestingly, 7,69 % of respondents already have the ISMS established and try to upgrade and improve this system. On average, enterprises reach M = 30,08 points; SD = 28,59 points. The data are skewed to smaller values (0,66) and are rather flat (-0,70). Up to 25 % of respondents reported a value of less than or equal to 2, meaning that these enterprises are not interested in the ISMS at all. The median represents only 24 points. 75 % of the values are up to 50 points. Overall, these data show that the enterprises do not initiate the ISMS and do not pay enough attention towards the ISMS. Since the data are not distributed according to the normal distribution (K–S test; Z = 1,47; p = 0,018), the 95 % confidence interval of the mean value cannot be reliably determined.

Figure 2 shows the evaluation of the ISMS3 variable in the surveyed enterprises. Most enterprises do not rate information security risks at all, up to 35,16 %. Following are enterprises that assess risks once a year (26,37 %) and twice a year (14,29 %). In general, the more often enterprises deal with the risks, the more they are prepared for possible threats and information security incidents. In our opinion, enterprises should assess the information security risks at least once a year. The survey shows 54,95 % of such enterprises. However, this percentage is surprisingly high for Slovakia, but still low compared to the potential impact of possible information security risks.

Fig. 2 Regularity of the information security risk assessment



Source: Authors' own research

The ISMS4 variable measures the perceived level of information security in the enterprise. Respondents on a scale from 0 (minimum) to 100 points (maximum) rated the information security level in their enterprise. The median is M = 62,93 points; SD = 27,68 points. The information security level in e–business is at 62,93 %. The enterprises claim that their level is sufficient. Due to the current information security threats, the level should be much higher. The respondents most frequently rated the level of information security by 80 points and the median is 70 points. Only 25 % of enterprises reach the level of less than or equal to 47,50 points. The data are more flat than spiked (-0,68), sloping to the right (-0,52) and not normally distributed (K–S test; Z = 1,63; p = 0,006). The information security level values could be explained in two ways. Either the information security is really at the sufficient level and the results reflect the real situation, or the enterprises lack adequate education and security awareness, while the respondents believe that the information security level of the enterprise is good.

According to the analysis results of the ISMS variables we conclude that enterprises are inclined to the need to improve ISMS, the enterprises currently do not pay enough attention to the ISMS according to the ISMS2 average value, most enterprises are concerned with evaluating information security risks and the enterprises also claim that their level of information security is sufficient. However, there is still a large group of enterprises that does not assess the information security risks and does not perform any ISMS activity.

4.1 Comparison of variables depending on the risk assessment

In the subchapter, we verify the difference between enterprises which assess information security risks (N = 59) and which do not assess the risks (N = 32). The groups are compared with values of individual variables ISMS1, ISMS2 and ISMS4 while testing whether the difference of groups is statistically significant. In the previous chapters we divided the variables into those from normal distribution (ISMS1) and those that are not normally distributed (ISMS2, ISMS4). The variables meeting the condition of data distribution normality are tested by the

independent samples t–test with equality of variances. By non–parametric Mann–Whitney U test, we test the variables that do not meet the normal distribution condition.

The following tables provide an overview of only those variables where have been demonstrated the statistical significance of the examined differences (ISMS1 and ISMS2). Table 4 shows Levene's test results that indicate the statistically significant difference in group variances ($F = 4,97$; $p = 0,028$). Subsequently, the t–test confirms the statistically significant difference in the ISMS1 (the need for the ISMS in the respondent's e–business) rating, $t (49,70) = 2,23$; $p = 0,030$, among those enterprises which assess information security risks ($M = 66,64$, $SD = 25,13$) and which do not assess the risks ($M = 51,06$, $SD = 34,05$).

Tab. 4 Testing differences of the ISMS1 variable depending on the risk assessment

		Levene's Test for Equality of Variances		T–test for Equality of Means						
									95 % Confidence Interval of the Difference	
	Equal variances	F	Sig.	t	df	Sig. (2–tailed)	Mean Difference	Std. Error Difference	Lower	Upper
ISMS1	Assumed	4,97	0,028	2,44	89,00	0,017	15,30	6,27	2,84	27,76
	Not assumed	–	–	2,23	49,70	0,030	15,30	6,85	1,54	29,06

Source: Authors' own research

The results of the non–parametric test in Table 5 show that enterprises dealing with information risks significantly differ in the enterprise's ISMS practice ($p < 0,05$) from enterprises that do not deal with the risks. The differences of the ISMS4 variable are random ($p > 0,05$).

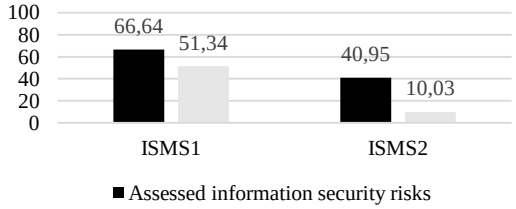
Tab. 5 Testing the differences of the ISMS2 variable depending on the risk assessment

Variable		Mann–Whitney U	Z	Asymp. Sig. (2–tailed)
ISMS2	Practicing the ISMS in the enterprise	328,00	-5,13	0,000

Source: Authors' own research

Figure 3 shows a summary of the surveyed variables with average values for each group with a statistically significant difference. Higher average values of variables are achieved in enterprises that assess information security risks. Differences between groups are evident and statistically significant according to the test results.

Fig. 3 Average values of groups in points with a statistically significant difference



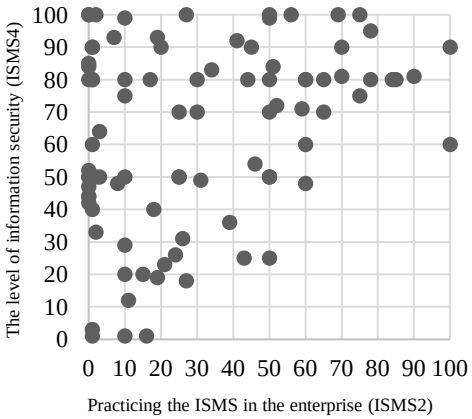
Source: Authors' own research

Enterprises that assess information security risks achieve a higher level of ISMS practice and emphasize the need for ISMS in their e–business more than enterprises that do not assess such risks.

4.2 Impact of practicing ISMS on the specified level of information security

By linear regression analysis, we verify the hypothesis whether the ISMS practice in the e–commerce enterprise (ISMS2) significantly affect the specified level of information security in that enterprise (ISMS4). We can observe a relationship of the variables in Figure 4, where the systematic linear dependence is not obvious, however, it cannot even be excluded.

Fig. 4 Correlation diagram of variables ISMS2 and ISMS4



Source: Authors' own research

The results of the regression are found in Table 6. The correlation coefficient ($R = 0,33$) demonstrates the weak interrelationship of the variables. The coefficient of determination ($R^2 = 0,11$) explains 11 % of variability of the dependent variable ISMS4 affected by the independent variable ISMS2. The remaining 89 % is influenced by other factors, such as investments in the ISMS, security controls, security training, incorporation of ISMS requirements into business processes, supply contracts, etc.

Tab. 6 Regression model of the dependent variable ISMS4 and the independent variable ISMS2

Model Summary (ISMS4)			
R	R Square	Adjusted R Square	Std. Error of the Estimate
0,33	0,11	0,10	26,30

ANOVA (ISMS4)					
	Sum of Squares	df	Mean Square	F	Sig.
Regression	7397,66	1	7397,66	10,70	0,002
Residual	61543,95	89	691,51	–	–
Total	68941,60	90	–	–	–

Coefficients (ISMS4)							
	Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95% Confidence Interval for B	
	B	Std. Error	Beta			Lower Bound	Upper Bound
Constant	53,40	4,01	0,00	13,31	0,00	45,42	61,37
SY2	0,32	0,10	0,33	3,27	0,002	0,12	0,51

Source: Authors' own research

Analysis of variance (ANOVA) confirms a statistically significant linear regression model with a good data description, $F (1, 89) = 10,70$; $p = 0,002$. The regression coefficient $b_1 = 0,32$ significantly contributes to the prediction of the ISMS4 variable ($p = 0,002$). Based on the results obtained, we reject the hypothesis H_0 and at the level of significance $\alpha = 0,05$ we accept

the alternative hypothesis H_1. The impact of the ISMS practice in an e–commerce enterprise on the enterprise's specified level of information security is statistically significant.

5 Discussion

The statement that enterprises in the Slovak electronic market lack a comprehensive system of information security management (Netolická, 2012; Král, 2011), was examined by the variable ISMS2. The results indicate (M = 30,08; SD = 28,59) that the statement is valid on our sample data. Up to 25 % of Slovak enterprises do not address the ISMS at all. It is clear from the data that the enterprises surveyed do not implement the ISMS, resp. only deal with the basic security measures. As a right path for enterprises, we propose a process application of the ISMS which will guarantee adequate information security of e–business. Only 8% of Slovak enterprises reach the advanced ISMS level. The remaining enterprises lack the comprehensive ISMS. However, according to the ISMS1 variable values, the respondents lean towards the need to improve the ISMS in their enterprise (M = 61,26, SD = 29,33). Up to 15,38 % of businesses are confident that the information security management system is needed. Therefore, the e–commerce enterprises are aware that practicing ISMS processes increases their information assets' security against risks, and at the same time increases the information security level in the enterprise. The fact that practicing the processes of such system has a statistically significant impact on increasing the information security level in the enterprise was proved by the results of the hypothesis verification.

6 Conclusion

We consider the information security management system a necessity for enterprises that want to successfully eliminate risks brought in by doing business in the electronic market. Businesses that use e–commerce to sell goods and services are particularly sensitive to customer trust. In the event of a successful security incident and subsequent disclose of this situation, a decline in customer trust may cause significant financial losses, mainly due to a decrease in orders. The ISMS as a comprehensive system within the overall e–business management can identify and eliminate information security risks in a timely manner. It is the ISMS processes' practice that increases the level of information security in the e–commerce enterprises. These enterprises consider the ISMS to be necessary, but they do not initiate the system. Enterprises that assess the information security risks practice the ISMS more and incline more towards the need for the ISMS in their e–business than enterprises that do not assess the risks at all.

Literature:

1. APEK: *Vývoj obratu v e-commerce od roku 2012*. [online]. 2017, [accessed 8.5.2018]. Available at: https://www.apek.cz/.
2. Cohen, K.: *Global ecommerce sales, trends and statistics 2016*. [online]. 2016, [accessed 8.5.2018]. Remarkety.com. Available at: https://www.remarkety.com/global-ecommerce-trends-2016.
3. Dvorský, J.: *Internetový predaj na Slovensku.* [online]. 2016, [accessed 8.5.2018]. Available at: http://www.bezpecnynakup.sk/storage/file/ts_19_10_16.doc.
4. ENISA a: *The ISMS Framework.* [online]. 2015, [accessed 8.5.2018]. Available at: https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-isms/framework.
5. ENISA b: *The Need for ISMS.* [online]. 2015, [accessed 8.5.2018]. Available at: https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-isms/need.
6. ESET: *Systém riadenia informačnej bezpečnosti.* [online]. 2014, [accessed 8.5.2018]. Available at: http://static1.esetstatic.com/uploads/media/System_riadenia_informacnej_bezpecnosti.pdf.
7. Hanák, R.: *Dátová analýza pre sociálne vedy*. Bratislava: Vydavateľstvo EKONÓM, 2016. 148 p. ISBN 978-80-225-4345-3.
8. HEUREKA: *Obrat e-commerce 2015.* [online] 2015, [accessed 8.5.2018]. Available at: https://www.heurekashopping.sk/resources/attachments/p0/20/heureka-obrat-2015-sk.jpg.
9. Ji, H., Zou, S.: Electronic Commerce in China Information Security Management System Strategy Research. In: *2nd International Conference on Humanities and Social Research (ICHSSR 2016)*. [online]. Singapore: Atlantis Press, 2016, [accessed 8.5.2018]. Available at: http://www.atlantis-press.com/php/download_paper.php?id=25861735.
10. Keith, M.: *Global ecommerce sales, trends and statistics 2015*. [online]. 2015, [accessed 8.5.2018]. Available at: http://www.remarkety.com/global-ecommerce-sales-trends-and-statistics-2015.
11. Klátiková, D., Gubová, K.: Kvalita elektronickej služby ako faktor zabezpečenia konkurencieschopnosti podniku. In *Manažment podnikania a vecí verejných - dialógy : vedecko-odborný časopis Slovenskej akadémie manažmentu.* Bratislava : Slovenská akadémia manažmentu, 2015. ISSN 1337-0510, 2015, 10 (30), pp. 97-107.
12. Kokles, M., Korček, F.: Analýza rizík informačnej bezpečnosti v malých a stredných podnikoch. In: *Ekonomika a manažment: Vedecký časopis Fakulty podnikového manažmentu Ekonomickej univerzity v Bratislave*. Bratislava: Fakulta podnikového manažmentu Ekonomickej univerzity v Bratislave, 2015. ISSN 1336-3301, 12 (1), pp. 38 – 55.
13. Kokles, M., Romanová, A.: *Informatika.* Bratislava: Sprint 2, 2014. 243 p. ISBN 978-80-89710-13-3.
14. Král, D.: Information Security in Small and Medium-Sized Companies. In: *ACTA VŠFS.* Praha: Vysoká škola finanční a správní, 2011. ISSN 1802-792X, 5 (1), pp. 61 – 73.
15. Laudon, K. C., Traver, C. G.: *E-commerce: business, technology, society*. 10th ed. New Jersey: Pearson, 2014. 905 p. ISBN 978-0133024449.
16. Li, D. C.: Online Security Performances and Information Security Disclosures. In: *Journal of Computer Information Systems*. Taylor & Francis, 2015. ISSN 0887-4417, 55 (2), pp. 20 – 28.
17. Lokhande, P. S., Meshram, B.: B. E-Commerce Applications: Vulnerabilities, Attacks and Countermeasures. In: *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*. 2013. ISSN 2278-1323, 2 (2), pp. 499 – 509.
18. Mohammadpourzarandi, M. E., Tamini, R.: The Application of Web Usage Mining In E-commerce Security. In: *7th International Conference on e-Commerce in Developing Countries: with focus on e-Security*. Kish Island: IEEE, 2013. pp. 1 – 8. ISBN 978-1-4799-0393-1.
19. Netolická, B.: *5 zásad pre riadenie a presadzovanie informačnej bezpečnosti v organizácii.* [online]. 2012, [accessed 8.5.2018]. Available at: http://www.eset.com/sk/firmy/services/clanky/5-zasad-informacnej-bezpecnosti/.
20. Ondrák, V., Sedlák, P., Mazálek, V.: *Problematika ISMS v manažerské informatice*. Brno: Akademické nakladatelství CERM, 2013. 378 p. ISBN 978-80-7204-872-4.
21. PCI SSC: *Information Supplement: PCI DSS E-commerce Guidelines.* [online]. 2013, [accessed 8.5.2018]. Available at: https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_eCommerce_Guidelines.pdf.
22. Said, A. R., et al.: Relationship between Organizational Characteristics and Information Security Knowledge Management Implementation. In: *Taylor´s 6th Teaching and Learning Conference 2013: Transformative Higher Education Teaching and Learning in Practice (TTLC 2013)*. Selangor: Taylor´s University, 2013. pp. 433 – 443.
23. Singh, A. N. et al.: Information Security Management (ISM) Practices: Lessons from Select Cases from India and Germany. In: *Global Journal of Flexible Systems Management*. Springer, 2013. ISSN 0972-2696. 14 (4), pp. 225 – 239.
24. Smith, S. N., Nah F. F., Cheng, M. X.: The Impact of Security Cues on User Perceived Security in e-Commerce. In: *Human Aspects of Information Security, Privacy, and Trust (HAS 2016)*. Cham: Springer, 2016. pp. 164 – 173. ISBN 978-3-319-39381-0.

25. Stehlíková, B., Horovčák, P.: *Manažment informačnej bezpečnosti v malých a stredných podnikoch*. [online]. 2012, [accessed 26.8.2017]. Available at: http://www.securityrevue.com/article/2012/06/manazment-informacnej-bezpecnosti-v-malych-a-strednych-podnikoch/.
26. STN ISO/IEC 27001: *Informačné technológie – Bezpečnostné metódy – Systémy riadenia informačnej bezpečnosti – Požiadavky*. Bratislava: Úrad pre normalizáciu, metrológiu a skúšobníctvo SR, 2014.
27. Yazdanifard, R., Edres, N. A. H., Seyedi, A. P.: Security and Privacy Issues as a Potential Risk for Further Ecommerce Development. In: *International Proceedings of Computer Science and Information Technology*. [online]. Singapore: IACSIT Press, 2011, 257 p. [accessed 26.8.2017]. Available at: http://www.ipcsit.com/vol16/5-ICICM2011M008.pdf.

Primary Paper Section: A

Secondary Paper Section: AE, BC