IBIMA Publishing
Journal of Innovation Management in Small & Medium Enterprises
https://ibimapublishing.com/articles/JIMSME/2023/441467/
Vol. 2023 (2023), Article ID 441467, 11 pages, ISSN: 2166-076X
DOI: 10.5171/2023.441467

Research Article

The Approaches to Information Security in Small and Medium-sized Companies in Slovakia: An Empirical Study

Benita BELÁŇOVÁ, Anna HAMRANOVÁ and Matej ČERNÝ

Department of Information Management, Faculty of Business Management,
University of Economics in Bratislava, Bratislava, Slovak Republic

Correspondence should be addressed to: Benita BELÁŇOVÁ; benita.belanova@euba.sk

Received date:31 October 2022; Accepted date:17 January 2023; Published date: 28 February 2023

Abstract

Securing information security is in the interest of all users of information and communication technologies, namely individuals, businesses and organizations, national authorities and institutions, multinational groups, and IT consulting companies. In this paper, we evaluate the results of our surveys in the field of information security in the sector of small and medium-sized enterprises, which were carried out in the years 2008 - 2020. The research was conducted through a research model that was developed based on the analyzed professional and scientific literature. The model was validated in the individual years of study on a sample of small and medium-sized enterprises operating in the Slovak Republic. The aim of the surveys was to map the evolution of the companies' approach to information security. Standard methods of scientific work such as analysis, synthesis, comparison, and selection were used in the preparation of the paper. A questionnaire survey was used to collect data, which were evaluated using descriptive statistics and cluster analysis. We expected that companies would pay more attention to information security during the study period, but this was not confirmed. In most cases, the values of the research indicators did not change in leaps and bounds, but gradually, and did not show large differences. The highest increase was recorded in the handling of sensitive information (23%), which can be justified by the regulation GDPR. Other positive values were in the following cases: personal data protection (an increase of 14%), problem management (an increase of 13%), and integration of information systems within the organization (an increase of 13%). We assumed that the main driver of increased care for information security would be legislative pressure in the Slovak Republic, but here we saw an increase of only 10%. An interesting and unexpected result was recorded in the case of small businesses, sector G - Trade - sales, consulting, services, which were classified into three different clusters. It means that small businesses operating in Slovakia in the same industry approach information security differently. A more detailed examination of the mentioned differences thus creates assumptions and topics for further research.

Keywords: information security, small and medium-sized businesses in Slovakia, research model and indicators, data mining

---

Cite this Article as: Benita BELÁŇOVÁ, Anna HAMRANOVÁ and Matej ČERNÝ (2023), "The Approaches to Information Security in Small and Medium-sized Companies in Slovakia: An Empirical Study", Journal of Innovation Management in Small and Medium Enterprise, Vol. 2023 (2023), Article ID 441467,
DOI: 10.5171/2023.441467

Introduction

Ensuring information security is in the interest of all users of information and communication technologies, namely individuals, businesses and organizations, institutions of individual countries, as well as multinational firms and IT consulting companies. Information and communication systems are such complex, extensive and interconnected systems that their smooth operation must be ensured by highly specialized personnel. However, these systems are often handled by lay users, threatened by human errors and mistakes, technical failures, natural elements, as well as targeted attacks, whether by disgruntled employees within the organization or by hackers and attackers from the outside. Businesses process most of the information they need to carry out their activities using information systems. A great deal of such information belongs under the governance of some legal standard of Slovak legislation, so even if the organization itself does not care that much about its data, they are obliged to protect them so that they do not come into conflict with the law.

Considering the impact of large organizations on the national economy, small and medium-sized enterprises appeared to be a not very interesting object of research and implementation of scientific knowledge. The change in this approach was caused by new trends brought about by globalization and computerization. Informatization also brought with it a new area that needs to be managed systematically, namely the security of information systems in the company.

In general, the security of information systems focuses mainly on the protection of information, the prevention and detection of unauthorized user and computer activity, as well as the protection of user privacy. With the spread of modern information and communication technologies into all areas of life, the importance of addressing data security in data collection, transmission, processing, and archiving has increased. This issue has been brought to the attention of managers mainly thanks to Act No. 122/2013 Coll. on the protection of personal data (in information systems) and Act No. 215/2004 Coll. on the protection of classified information and their subsequent amendments. However, the issue is much broader. The importance attached to information security is also evidenced by the ever-growing interest of companies in designing, enforcing, and implementing a security policy.

To verify the state of information security in the conditions of small and medium-sized enterprises in the Slovak Republic, we conducted a survey. The main objective of the survey was to identify the threats affecting information systems, ways of dealing with information security, and the most serious obstacles to the enforcement of security policy.

Most research studies, whether global or local, confirm the increasing number of attacks on enterprise IS/IT, the growing number of security incidents, and point to the weak readiness of enterprises to comprehensively address information security. Preparedness is not only about the securing of information and information systems, but also about the management approach and the necessary staff training. TÜV SÜD (2021) states that up to 80% of leaks are caused by human factors and another 20% by external attacks. A comparison of companies operating abroad and in Slovakia also comes out unfavorably in the field of information security for companies in Slovakia (Yar, 2021).

These facts led us to summarize the results of our own surveys in the field of information security in the sector of small and medium-sized enterprises in Slovakia carried out in the years 2008 - 2020.

Literature Review

The issue of ensuring information security is a widely elaborated topic in domestic and foreign literature. In the Slovak Republic, the approach to information security is addressed by the Alfapro portal (2021), which characterizes information security as a problem for all enterprises regardless of their size. The difference is that the larger the company is, the more extensive the opportunities it has to acquire experts, which also applies in the field of information technology. Large companies usually have their own IT departments, which are assisted by external contractors according to the current needs. This will ensure that the company has a sufficient range of experts in the different areas of IT and in the field of information security. Small, but also some medium-sized, enterprises do not have such extensive resources. In their case, the area of IS/IT care is rather related to one person who, among other duties, is also in charge of IT. In the best case, such a company hires an IT outsourcing company.

Ensuring the security of enterprise IS/IT infrastructure is an ongoing process that is standardized by the ISO/IEC 27000 series of standards. These standards are international standards in the field of information security management derived from the British Standards BS 7799 series (CSIRT.SK, 2021). IS/IT security in enterprises is largely influenced by legislation and case law. In Slovakia, at the national level, information security is mainly covered by Act No. 18/2018 Coll. on the Protection of Personal Data (GDPR) (ÚOOS SR, 2018) and Act No. 69/2018 Coll. on Cyber Security (Slov-Lex, 2018).

The importance of the human factor, the focus on the SME sector, as well as the respect of norms, standards, and legislation in ensuring information security are also underlined by the research of foreign authors.

Authors Sanchez, et al. (2009) dealt with the methodology of information security management in small and medium-sized enterprises. They presented a methodology for the management of security and its maturity in SMEs and justified its applicability in practice. This methodology is composed of three main subprocesses: GEGS – Generation of Security Management Schemas, GSGS – Generation of Security Management Systems, and MSGS – Maintenance of the Security Management System.

A team led by Sanchez published the Implanted Security Culture (ISC) model in 2010 (Sanchez, et al., 2010). The objective of the process is to evaluate any user who wishes to access the company's information system regarding his/her knowledge of the ISMS's regulations, in order to determine whether s/he is suitably prepared to access this system.

Kaur and Mustafa (2013) investigated the impact of knowledge, attitudes, and approaches toward information security in SMEs in Malaysia. Their findings represent employees' information security awareness, indicating those attitudes and behaviors that significantly affect the confidentiality, integrity, and availability of business information.

Els and Cillers (2015) identified 6 key factors and 4 pillars of information security assurance in South Africa. The pillars of IB are: protection, detection, recovery, and compliance, and the key factors are: top management commitment, employee and user awareness/training, access control, infrastructure security, third-party security, security policies, and regular assessment.

Mijnhardt, Baars and Spruit (2016) – proposed Characterizing Organizations' Information Security for SMEs (CHOISS) model. This model relates 4 categories (A–D), 11OCs (1–11), and 47 measurement levels. They proposed prerequisites for ensuring information security (which are often neglected in SMEs). These are: skilled workforce, documented processes, and IT budget planning. Skrodelis, et al. (2020) examined information security from the perspective of COBIT methodology.

For our research, we have designed our own model of research indicators, which we have gradually verified in small and medium-sized enterprises in Slovakia.

Research Framework and Methodology

The research framework, in addition to the literature study, consisted of the formulation of the main goal of the paper, the sub-goals and the methods used, the design of the model of research indicators, the implementation of questionnaire surveys, their evaluation, and the formulation of conclusions and recommendations.

The main goal of the paper was to map the development in the area of the approach to information security in the SME sector in Slovakia. In addition to the literature review, our research between 2008 and 2020 was conducted through questionnaire surveys in individual years based on the research indicator model. The model of research indicators was created based on published scientific works in the field of information security at home and abroad. The respondents were managers of small and medium-sized enterprises operating in Slovakia, while the research model was focused on the assessment of the importance of information security in the enterprise in which they work.

The following sub-goals were set to support the main goal:

- analysis of relevant scientific literature,
- creating a research model,
- creation and evaluation of a questionnaire survey concerning the assessment of the implementation of information security in enterprises in Slovakia
- formulation of the conclusions.

We present the research model and the significance of each indicator along with the results in Table 1.
Descriptive statistics and contingency tables, cluster analysis (to identify similar or dissimilar groups of data), were used to evaluate the results. Cluster analysis was performed using WEKA software (Hall et al., 2009).

Research Sample

The research was carried out based on questionnaire surveys in 2008, 2012, 2015, 2017, and 2020 in small and medium-sized enterprises in Slovakia. The research involved 202 enterprises in 2008, 129 in 2012, 183 in 2015, 219 in 2017, and 248 in 2020. The representation of SME enterprises ranged between 40% - 60% each year. By legal form, limited liability companies had the largest representation. According to the ownership structure, enterprises with exclusively domestic ownership or with dominant domestic ownership prevailed. Of the industries (according to SK NACE), the largest number of enterprises in the research sample were in the category G - Trade - Sales, Consulting, Services, and C - Manufacturing industries. The research sample is shown in Table 1.

Table 1: Research Sample

Parameter	Parameter value	2008	2012	2015	2017	2020
P1 – Company size	small (10 – 49 employees)	54%	58%	60%	61%	56%
	medium (50 – 249 employees)	46%	42%	40%	39%	44%
P2 – Legal form	state-owned enterprise	7%	4%	3%	3%	3%
	public limited company	19%	21%	14%	20%	18%
	company with limited liability	62%	61%	72%	73%	76%
	cooperative	4%	2%	0%	1%	2%
	trades	7%	8%	4%	3%	2%
P3 – Ownership structure	100% share of state ownership	6%	7%	7%	3%	3%
	dominant domestic owner	10%	26%	13%	11%	10%
	dominant foreign owner	9%	9%	7%	14%	13%
	exclusively domestic owner	62%	37%	48%	51%	52%
	exclusively foreign owner	12%	21%	26%	21%	21%
P4 – Industry (According to SK NACE)	D - Supply of electricity, gas, and steam	1%	2%	3%	2%	2%
	H - Transportation and storage	4%	3%	4%	3%	2%
	J - IT, telecommunications	14%	17%	16%	17%	17%
	G - Trade - sales, consulting, services	32%	24%	31%	22%	25%
	S - Other activities	6%	16%	15%	25%	24%
	A - Agriculture, forestry, and fishing	3%	2%	1%	2%	2%
	F - Construction industry	11%	9%	6%	9%	8%
	I - Tourism - Accommodation and catering services	3%	2%	3%	8%	4%
	O - Public, state administration, and defense	4%	4%	3%	2%	2%
	C - Industrial production	25%	24%	20%	22%	13%

(Source: Authors' own)

Results and Discussion

We present the results of the research in the following structure: the results of the individual indicators according to the research model (% response rates - Table 2) and the results of the cluster analysis (Table 3).

Results of the evaluation of research indicators

Table 2: Research model including evaluation of individual indicators

Indicator	Indicator value	2008	2012	2015	2017	2020	Difference (2020 – 2008)
VIB1 The organization's management is familiar with IS security regulations	yes	62%	59%	63%	62%	63%	1%
	partially	35%	38%	34%	30%	32%	-3%
	no	3%	2%	3%	8%	5%	2%
VIB2 IS strategy is in line with the organization's strategy	Yes	57%	62%	55%	64%	68%	11%
	no	43%	38%	45%	36%	32%	-11%
VIB3 The importance of information security in terms of the organization's objectives	high importance	53%	58%	56%	57%	58%	5%
	medium importance	38%	36%	36%	33%	32%	-6%
	small importance	9%	5%	9%	11%	10%	1%
VIB4 Sufficient attention is dedicated to the practical implementation of information security assurance	yes	75%	77%	81%	76%	80%	5%
	no	25%	23%	19%	24%	20%	-5%
VIB5 Level of information security in the organization	excellent level	20%	23%	26%	28%	29%	9%
	good level	66%	65%	63%	57%	61%	-5%
	low level	13%	12%	10%	14%	9%	-4%
	insufficient level	0%	0%	2%	1%	1%	1%
VIB6 The level of employees' perception of the quality of IT services in the organization	full satisfaction	53%	51%	52%	54%	52%	-1%
	partial satisfaction	44%	47%	48%	44%	44%	0%
	dissatisfaction	3%	2%	1%	2%	4%	1%
VIB7 Circumstances affecting information security enforcement	VIB71 personal data protection	78%	80%	88%	98%	92%	14%
	VIB72 integration of information systems outside the organization	46%	45%	49%	58%	41%	-5%
	VIB73 integration of information systems within the organization	24%	50%	45%	36%	37%	13%
	VIB74 rapid IT developments	46%	20%	46%	25%	26%	-20%
	VIB75 customer pressure/requirements	23%	22%	34%	6%	26%	3%

	VIB76 requirements for mobile information processing	21%	23%	27%	17%	14%	-7%
	VIB77 pressure/requirements of business partners	22%	27%	27%	22%	24%	2%
	VIB78 legislative pressure in Slovakia	16%	22%	24%	25%	26%	10%
	VIB79 e-business and/or e-commerce	17%	12%	18%	15%	19%	2%
	VIB780 current and upcoming EU legislation	16%	8%	13%	8%	14%	-2%
	VIB781 pressure/requirements from investors/shareholders/owners	14%	12%	13%	11%	14%	0%
	VIB782 results of the performed audit/recommendation of the IS/IT auditors	12%	13%	9%	20%	20%	8%
	VIB783 other reasons	2%	1%	1%	0%	2%	0%
VIB8 Scope of the security policy (% of yes responses)	VIB81 network security (including Internet)	65%	70%	85%	95%	74%	9%
	VIB82 security personal computers	52%	56%	67%	77%	64%	12%
	VIB83 operation of information systems	58%	47%	58%	67%	58%	0%
	VIB84 handling sensitive information	46%	33%	50%	62%	69%	23%
	VIB85 physical security	56%	47%	43%	37%	51%	-5%
	VIB86 disaster recovery planning	36%	24%	35%	36%	41%	5%
	VIB87 staffing (including training)	26%	33%	29%	40%	27%	1%
	VIB88 responses to security incidents	22%	16%	19%	22%	31%	9%
	VIB89 software development	25%	14%	18%	28%	24%	-1%
	VIB810 logical security	30%	11%	17%	18%	19%	-11%
	VIB811 third-party services	12%	17%	15%	26%	27%	15%
	VIB812 program change management	18%	8%	12%	15%	16%	-2%
	VIB813 problem management	9%	12%	19%	11%	22%	13%

(Source: Authors' own)

The percentages of scores for each indicator can be seen in Table 2. We expected that the % shares of respondents' answers will increase within the indicators of the research model over the years towards increased awareness of information security and will decrease in the indicators with negative attitudes towards this issue. The answers in the case of most indicators did not change suddenly, but gradually. Interesting differences were noted for indicator VIB2 (answer yes), where there was an increase of 11%, for indicator VIB71 (answer yes), an increase of 14%, VIB73 an increase of 13%, VIB78 an increase of 10%, indicator VIB82 an increase of 12%, VIB84 an increase of 23%, VIB811 an increase of 15%, VIB813 an increase of 13%. It means that the evaluation of the approach to the IS strategy in accordance with the organization's strategy has increased by 11%. Of the circumstances affecting the enforcement of information security, the largest increase was recorded in access to personal data protection (an increase of 14%), integration of information systems within the organization (an increase of 13%), and legislative pressure in the Slovak Republic (an increase of 10%). In the group of indicators related to the scope of the security policy, the following indicators noted increases: securing personal computers (up 12%), handling sensitive information (up 23%), third-party services (up 15%), and problem management (up 13%).

Only the decline in VIB85 (down 5%) and VIB 810 (down 11%) can be assessed negatively. These declines mean that respondents rate the scope of physical security policy in 2020 as 5%

lower than in 2008. Similar is the case for logical security, where there is a drop of up to 11%.

In the case of the other indicators, we note little variation, which can be considered as stagnation.

Cluster analysis results

The results of the cluster analysis are shown in Table 3. The highest and lowest mean values of the indicators, as well as the overall means in each cluster, are highlighted in bold.

We used the Simple K-means algorithm by solving cluster analysis (It groups related values, which are different from other clusters, into individual clusters). We gradually varied the number of clusters from 2 to 5 and recorded the resulting scores of indicators VIB1, ... VIB813. An even distribution of the research sample was for the 5 clusters, so we selected these results for reporting. The Full Data column shows the average values of the whole sample (all Clusters), and the other columns group the values of the individual Clusters identified by the Simple K-means algorithm.

Table 3: Results of cluster analysis

Attributes	Full Data	Cluster 0	Cluster 1	Cluster 2	Cluster 3	Cluster 4
	100%	13%	23%	27%	20%	17%
P1 - Company size	small	small	small	medium	small	small
P2 – Legal form	Ltd.	Ltd.	Ltd.	Ltd.	Ltd.	Ltd.
P3 - Ownership structure	exclusively domestic owner	exclusively domestic owner	exclusively domestic owner	exclusively foreign owner	exclusively domestic owner	exclusively domestic owner
P4 - Industry	G	G	G	J	G	S
VIB1	1.58	1.55	1.77	1.65	1.04	1.85
VIB2	0.68	0.7	0.9	0.75	0.12	0.9
VIB3	1.48	1.58	1.72	1.53	0.84	1.73
VIB4	0.8	0.97	0.93	0.81	0.35	1
VIB5	**2.17**	**2.33**	**2.33**	**2.29**	**1.67**	**2.22**
VIB6	1.48	1.7	1.5	1.4	1.33	1.63
VIB71	0.92	0.85	0.9	0.93	0.94	0.98
VIB72	0.41	0.3	0.81	0.46	0.08	0.27
VIB73	0.37	0.45	0.4	0.37	0.22	0.44
VIB74	0.26	0.42	**0.04**	0.31	0.24	0.37
VIB75	0.25	0.79	0.09	0.24	0.16	0.17
VIB76	0.15	0.18	0.09	0.13	0.08	0.29
VIB77	0.23	0.64	0.21	0.18	0.06	0.22
VIB78	0.26	0.24	0.07	0.29	0.16	0.61
VIB79	0.14	0.24	0.12	0.19	**0.02**	0.12
VIB780	0.14	0.3	0.12	0.18	**0**	0.15
VIB781	0.18	0.12	0.12	0.37	0.06	0.15
VIB782	**0.02**	**0.03**	**0.04**	**0.01**	0.04	**0**
VIB783	0.19	0.4	0.09	0.22	0.12	0.2
VIB81	0.74	0.55	0.84	1	0.53	0.56
VIB82	0.19	0.15	0.05	0.44	0.04	0.15
VIB83	0.27	**0.06**	0.32	0.54	0.1	0.1

VIB84	0.16	**0.03**	0.05	0.46	**0**	0.12
VIB85	0.22	0.21	0.21	0.21	0.2	0.27
VIB86	0.64	0.88	0.6	0.93	0.43	0.3
VIB87	0.58	0.3	0.63	0.94	0.29	0.46
VIB88	0.69	0.45	0.61	0.93	0.55	0.73
VIB89	0.51	0.45	0.39	0.87	0.24	0.46
VIB810	0.41	0.27	0.35	0.84	0.12	0.22
VIB811	0.27	0.18	0.18	0.5	0.16	0.22
VIB812	0.31	0.09	0.21	0.76	0.14	**0.05**
VIB813	0.24	**0.03**	0.39	0.32	0.14	0.2

(Source: Authors' own)

Cluster 0 is made up of 13% small businesses, legal form Ltd., exclusively domestically owned, operating in industry G - Trade - sales, consulting, services.

Cluster 1 is made up of 23% of businesses characterized in the same way as cluster 0, i.e., small businesses, exclusively domestically owned enterprises operating in the G - Trade - sales, consulting, services.

Cluster 2 consists of 27% of medium-sized enterprises, legal form Ltd., exclusively foreign-owned, operating in the industry J - IT, telecommunications.

Cluster 3 is made up of 20% of small businesses, legal form Ltd., exclusively domestically-owned, operating in the industry G - Trade - sales, consulting, services.

Cluster 4 consists of 17% of small businesses, legal form Ltd., exclusively domestically-owned, operating in the industry S - Other activities.

Cluster analysis showed that the highest ranked research indicator in all clusters was indicator VIB5 - Level of Information Security in the organization, which we evaluate positively, as respondents declare an increasing level of Information Security in their companies/organizations.

The lowest values were recorded for indicators VIB7 - circumstances affecting information security enforcement and VIB8 - scope of the security policy. Specifically, these variables are VIB74 - rapid IT developments (lowest value in cluster 1), VIB79 - e-business and/or e-commerce (lowest value in cluster 3), VIB782 - results of the performed audit/recommendation of the IS/IT auditors (lowest value in clusters full data, clusters 0,1,2 and 4) and VIB783 - other reasons (lowest value in cluster 0). The scope of the security policy (variable VIB8) reached the lowest values for the variable VIB812 - program change management (in cluster 4) and VIB813 - problem management (in cluster 0).

Interestingly, the differently classified small businesses, exclusively domestically-owned, industry G Trade - sales, consulting, services, which are classified in three different clusters (clusters 0, 1, and 3). When examining the differences of the above clusters from the mean (cluster full data), we focused on calculating the difference in the values of the individual indicators from the mean (Table 4). Cluster 1 (23% of enterprises) is the least different from the average, with an average deviation of MEAN = 0.004, VAR = 0.29, STDEV = 0.54. This is followed by cluster 0 (13% of businesses) with MEAN = 0.016, VAR = 0.28, STDEV = 0.53. The largest differences from the mean were observed in cluster 3 (20% of enterprises), namely: MEAN = -0.202, VAR = 0.22, STDEV = 0.47.

Table 4: Comparison of selected clusters

Attributes	Full Data	Cluster 0	Differences from the average	Cluster 1	Differences from the average	Cluster 3	Differences from the average
	100%	13%		23%		20%	
P1 - Company size	small	small		small		small	
P2 – Legal form	Ltd.	Ltd.		Ltd.		Ltd.	
P3 - Ownership structure	exclusively domestic owner	exclusively domestic owner		exclusively domestic owner		exclusively domestic owner	
P4 - Industry	G	G		G		G	
VIB1	1.58	1.55	-0.03	1.77	0.19	1.04	-0.54
VIB2	0.68	0.7	0.02	0.9	0.22	0.12	-0.56
VIB3	1.48	1.58	0.1	1.72	0.24	0.84	-0.64
VIB4	0.8	0.97	0.17	0.93	0.13	0.35	-0.45
VIB5	2.17	2.33	0.16	2.33	0.16	1.67	-0.5
VIB6	1.48	1.7	0.22	1.5	0.02	1.33	-0.15
VIB71	0.92	0.85	-0.07	0.9	-0.02	0.94	0.02
VIB72	0.41	0.3	-0.11	0.81	0.4	0.08	-0.33
VIB73	0.37	0.45	0.08	0.4	0.03	0.22	-0.15
VIB74	0.26	0.42	0.16	0.04	-0.22	0.24	-0.02
VIB75	0.25	0.79	0.54	0.09	-0.16	0.16	-0.09
VIB76	0.15	0.18	0.03	0.09	-0.06	0.08	-0.07
VIB77	0.23	0.64	0.41	0.21	-0.02	0.06	-0.17
VIB78	0.26	0.24	-0.02	0.07	-0.19	0.16	-0.1
VIB79	0.14	0.24	0.1	0.12	-0.02	0.02	-0.12
VIB780	0.14	0.3	0.16	0.12	-0.02	0	-0.14
VIB781	0.18	0.12	-0.06	0.12	-0.06	0.06	-0.12
VIB782	0.02	0.03	0.01	0.04	0.02	0.04	0.02
VIB783	0.19	0.4	0.21	0.09	-0.1	0.12	-0.07
VIB81	0.74	0.55	-0.19	0.84	0.1	0.53	-0.21
VIB82	0.19	0.15	-0.04	0.05	-0.14	0.04	-0.15
VIB83	0.27	0.06	-0.21	0.32	0.05	0.1	-0.17
VIB84	0.16	0.03	-0.13	0.05	-0.11	0	-0.16
VIB85	0.22	0.21	-0.01	0.21	-0.01	0.2	-0.02
VIB86	0.64	0.88	0.24	0.6	-0.04	0.43	-0.21
VIB87	0.58	0.3	-0.28	0.63	0.05	0.29	-0.29
VIB88	0.69	0.45	-0.24	0.61	-0.08	0.55	-0.14
VIB89	0.51	0.45	-0.06	0.39	-0.12	0.24	-0.27
VIB810	0.41	0.27	-0.14	0.35	-0.06	0.12	-0.29
VIB811	0.27	0.18	-0.09	0.18	-0.09	0.16	-0.11
VIB812	0.31	0.09	-0.22	0.21	-0.1	0.14	-0.17
VIB813	0.24	0.03	-0.21	0.39	0.15	0.14	-0.1

MEAN	**0.529**	**0.545**	**0.016**	**0.534**	**0.004**	**0.327**	**-0.202**
VAR			**0.28**		**0.29**		**0.22**
STDEV			**0.53**		**0.54**		**0.47**

(Source: Authors' own)

Conclusion

The main goal of the paper was to map the development in the approach to information security in the SME sector in Slovakia. Enterprises operating in Slovakia are not at the forefront of information security in Europe, so we have made the research more general and focused on the evaluation of the indicators of our proposed research model. The results showed that, in most cases, the values of the research indicators did not change suddenly but gradually and did not show high variation, as might be expected. The highest increase in the surveyed period was observed in the handling of sensitive information (23%), which can be justified by the GDPR. Other positive values were in the cases of approach to personal data protection (an increase of 14%), problem management (an increase of 13%), and integration of information systems within the organization (an increase of 13%). We expected legislative pressure in the Slovak Republic to be the main driver of increased attention to information security, but here we noted an increase of only 10%. We consider the decline in VIB85 (a decrease of 5%) and VIB810 (a decrease of 11%) to be negative. These declines mean that respondents rate the scope of physical security policy in 2020 as 5% lower than in 2008. Similar is the case for logical security, where there is a drop of up to 11%. In the case of the other indicators, we note little variation, which can be considered as stagnation.

Based on the cluster analysis, in addition to a more detailed assessment of the values of the individual variables (Results and Discussion chapter), we observed an unexpected result in the case of small businesses, legal form Ltd., exclusively domestically owned, industry G Trade - sales, consulting, services, which were classified into three different clusters with different values of the examined indicators, namely 13% of the enterprises into cluster 0, 23% of the enterprises into cluster 1, and 20% of the enterprises into cluster 3. This fact means that small businesses operating in Slovakia in the same industry approach information security differently. This created the preconditions for their more detailed examination and the ideas for further research.

Acknowledgments

The paper was elaborated within VEGA No. 1/0388/20 IT Management in Enterprises in Slovakia: International Standards and Norms Versus Individual Business Processes – proportion 100 %.

References

- Alfapro. (2019). 'IT Riešenia' [Online], [Retrieved November 05, 2021], https://www.alfapro.sk/pristup-k-informacnej-bezpecnosti-v-malych-a-strednych-podnikoch/.
- CSIRT.SK. (2021). 'Štandardy informačnej bezpečnosti' [Online], [Retrieved November 25, 2021], https://www.csirt.gov.sk/standardy-informacnej-bezpecnosti.html.
- Els, F., Cilliers, L. (2015). 'Improving the information security in SMEs to protect customer's personal identifiable information'. *Journal of Business and Management Dynamics* 5(1), 75 – 79, http://dx.doi.org/10.4102/ jbmd.v5i1.7.
- Kaur, J. and Mustafa, N. (2013). 'Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME'. *In 2013 International Conference on Research and Innovation in Information Systems (ICRIIS)*, 286-290.
- Mijnhardt, F., Baars, T., Spruit, M. (2016). 'Organizational characteristics influencing SME information security maturity', *Journal of Computer Information Systems*, 56(2), 106-115.
- Sánchez, L. E., Parra, A. S. O., Fernández-Medina, E., Piattini, M. (2009). 'MMSM-SME: Methodology for the management of security and its maturity in Small and Medium-sized Enterprises'. *In 11th International Conference on Enterprise Information Systems (WOSIS09*), Milan, Italy, 67-78.
- Sánchez, L. E., Santos-Olmo, A., Fernández-Medina, E., Piattini, M. (2010). 'Security culture in small and medium-size enterprise'. *In International Conference on ENTERprise Information Systems*, Springer, Berlin, Heidelberg, 315-324.

- SK NACE (2022). 'NACE codes'. [Online], [Retrieved November 25, 2008], http://www.nace.sk/.
- Skrodelis, H. K., Strebko, J.,Romanovs, A. (2020). 'The Information System Security Governance Tasks in Small and Medium Enterprises'. *In 2020 61st International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS*), 1-4.
- Slov-Lex. (2018). 'Act 18/2018 on personal data protection and amending and supplementing certain Acts'. [Online], [Retrieved January 25, 2022], https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/.
- TÜV SÜD Journal (2021). 'Informačná bezpečnosť je zodpovednosťou celej organizácie'. [Online], [Retrieved March 15, 2022], https://www.tuvsud.com/sk-sk/informacne-centrum/tuv-sud-journal/sk/informacna-a-kyberneticka-bezpecnost/informacna-bezpecnost-je-zodpovednostou-celej-organizacie.
- Úrad na ochranu osobných údajov Slovenskej republiky (ÚOOS SR). (2018). 'Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov publikovaný v Zbierke zákonov SR'. [Online], [Retrieved January 15, 2022], https://dataprotection.gov.sk/uoou/sk/content/zakon-c-182018-z-z-o-ochrane-osobnych-udajov-o-zmene-doplneni-niektorych-zakonov-publikovany.
- Yar, L. (2021). 'Dáta sú ropou 21. storočia. Ako sa o ne stará Slovensko?'. [Online], [Retrieved January 15, 2022], https://euractiv.sk/section/digitalizacia/news/data-su-ropou-21-storocia-ako-sa-o-ne-stara-slovensko/.