ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2019 Volume 6 Number 4 (June)
http://doi.org/10.9770/jesi.2019.6.4(37)

Publisher
http://jssidoi.org/esc/home

INFORMATION SECURITY MANAGEMENT IN SMES: FACTORS OF SUCCESS

Aleksandr Ključnikov[1], Ladislav Mura[2], David Sklenár[2]

[1] University of Entrepreneurship and Law, Prague, Czech Republic
[2,3] Pan-European University, Faculty of Economics and Business, Bratislava, Slovakia

E-mails:[1] kliuchnikov@gmail.com ; [2]ladislav.mura@paneurouni.com , [3]davids@itcom.sk

Received 20 February 2019; accepted 16 May 2019; published 30 June 2019

Abstract. While the consecutive metamorphoses in the world economy changes the paradigm of doing business, the sources of success of almost every type of business transfer from tangible to intangible assets, and the information and its value becomes more and more significant, especially in the segment of small and medium sized enterprises. The aim of this paper was to identify the factors of success of information security management in segment of SMEs in Slovakia. Based on the literature research we identified 4 main factors of success of information security management, including the Compliance of information security management with the company's business activities, Support of top management, Security controls and Organizational awareness. To identify the importance and interconnections of the specified factors we have addressed senior IT security experts from SMEs in Slovakia. The experts evaluated the significance and relationships the factors of success of information security management and the results of the expert evaluation were processed using the DEMATEL technique. The results of the research show that the Security Controls and Supportive top management are the most important factors in general, while the factor of organizational awareness is the most obvious and important in the short-term period. Our results imply that SMEs should promote organizational awareness in information security management in line with implementation of the security controls at the first line of the defense.

Keywords: information security management; DEMATEL; support of top management; security controls; organizational awareness

Reference to this paper should be made as follows: Ključnikov, A.; Mura, L.; Sklenár, D. 2019. Information security management in SMEs: factors of success, *Entrepreneurship and Sustainability Issues* 6(4): 2081-2094. http://doi.org/10.9770/jesi.2019.6.4(37)

JEL Classifications: D80, M15, 032

1. Introduction

While the consecutive metamorphoses in the world economy changes the paradigm of doing business, the sources of success of almost every type of business transfer from tangible to intangible assets, and the information and its value becomes more and more significant. Belan (2015) state that information becomes the most important competitive assets of the company and that information becomes a high market value goods. Khouri (2009) confirms that information is one of the most important assets that organizations have, and therefore, it needs the protection which is adequate to its value.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2019 Volume 6 Number 4 (June)
http://doi.org/10.9770/jesi.2019.6.4(37)

Sklenár and Čimová (2018) declare that however, the progress in the development of the digital economy is crucial for the improvement of the competitiveness of the EU economy, the use of ICT is also highly associated with threats. Information currently became a potential target for threats and needs to be protected. While information itself is a type of intangible capital its value is not easy to assess. However, traditional performance measurement methods focus on known financial measures, they are not satisfactory to describe and manage intangible information assets (Huang et al., 2006). Polkowski and Dysarz (2017) note that the interest in aspects of information security management for researchers, traders and users is increasing.

It is generally known that small and medium-sized enterprises (SMEs) are one of the most important and valuable part of the world economy (Badulescu, 2010; Karpak and Topcu, 2010; Maciejewski and Wach, 2019), and as the most important engine of an economic growth (Henderson and Weiler, 2010). 99 % of all companies in the USA and the European Union belong to a category of SMEs (Bhaird, 2010; Peracek at el., 2018). Slovak economy, where our research takes place, is not an exception. The share of SMEs in this country reaches is 99.9 % of the total number of enterprises, their share of the state's value added is about 53 % (Slovak business agency, 2015). According to the same data source SMEs employ more than 72% of labor force in this country.

However, Verbano and Venturini (2013) insist that all enterprises need to adopt risk management strategy and methodology to identify, assess and treat risks to survive on the market, only large enterprises do usually have a well-developed risk management and are applying risk limiting instruments, while SMEs do not often know that these instruments even exist (Belás et al., 2014). The research in the field of risk management by Adásková (2009) confirmed that 76% of SMEs usually address the risk via an intuitive approach, and only 36.5% of them uses risk management systems. While SMEs belong to the most vulnerable business segment, underestimation of the risks in the field of information security management may be crucial for these enterprises.

The aim of this paper is to identify the factors of success of information security management in segment of SMEs in Slovakia. The paper has the following structure. The first chapter brings the results of the literature research on the topic of information security management. The second chapter presents the applied methodology together with the description of the key factors of information security management. The third chapter presents the results of the case study, and the last chapter brings a shorts discussion and conclusion of the study.

2. Literature review

Information security is one of the key areas of organizational security management. Security Management is a field of management that addresses the security of assets in an enterprise. According to Khouri (2009), information security means the protection of information during its creation, processing, storage, transmission and disposal, through logical, technical, physical and organizational measures that counteract the loss of confidentiality, integrity and availability. Information security management is according to ISO / IEC 2000: IT service management a "set of tools and measures ensuring the security of information and their flows in the company".

Information Security Management is a part of the overall organization management system, the foundation for managing security risks, the goal of which is to establish, implement, operate, monitor, review, maintain and improve information security in the organization (Rajnoha et al., 2017; Radu, 2018; Davidekova et al. 2016; Lengyel et al., 2017; Tvaronavičienė, 2018; Davidavičienė et al., 2019).

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2019 Volume 6 Number 4 (June)
http://doi.org/10.9770/jesi.2019.6.4(37)

According to the same authors the organization's management should establish a clear information security policy orientation in line with the organization's objectives and demonstrate support for, and commitment to, information security through the publication and maintenance of an information security policy across the organization.

Hudec (2014), Gródek-Szotak and Nesterak (2017) or Korenkova et al. (2019) declare that the information security policy document should be approved by the management of the organization and should contain opinions on the definition of information security, its overall purpose and scope, its importance as a mechanism for sharing information.

According to Dekýš (2010), small and medium-sized enterprises form a specific environment in terms of enforcement and information security management. The differences with large companies are as follows (Dekýš, 2010): *non-existing or just a minimal security team; missing budget for information security, or a budget as a part of the general IT budget; lower range of financial, time and human resources allocated to information security; use of the open-source projects to minimize ITC expenditures; security management performed by the IT department.*

According to Millaire et al. (2017), Mandorf and Gregus (2014), Zavadska and Zavadsky (2018) a fundamental reason why SMEs are a popular target for threats is that attackers are looking for simple goals and small companies with limited budgets and don't consider cyber security to be important. SMEs they are easier to disrupt than large enterprises that invest substantial amount of funds in the security of information systems (Millaire et al., 2017).

Hau et al. (2016) note that most companies do not know for months that they have been attacked. According to FireEye (2016), most companies were not able to identify for months that they were attacked (469 days on average since the incident after detection). FireEye (2016) also stated that while the media mostly present the information about the data breaches of the giant corporations, as many as 77% of cybercrime is actually targeting SMEs.

Most cyberattacks on small and medium-sized enterprises (SMEs) are the result of a bad password (Ashford, 2017). Some password management suggestions are also presented by Chmielarz and Zborowski (2017).
For the successful implementation of security policy, critical factors need to be identified and the level of importance of each one assessed. The study by Lopesa and Oliveira (2015) or Vilcekova et al. (2018) contributes to the identification of these factors by presenting the results of a survey of security of information systems in SMEs. The aim of the study by Tu and Yuan (2014) was to identify the factors of successful implementation of information security management in an enterprise. Based on the twenty most relevant and recent studies, they identified ten factors that may be considered important in implementing information security management. The most important factors in determining the successful implementation of information security management are *employee awareness and training*, as well as the *support for senior management*. The importance assessment for both specified factors is almost the same.

Tu, et al. and (2018) and Olah et al. (2019) focused the study on identifying and modeling factors that contribute to the success of information security management. They identified six critical success factors. The authors concluded that, through business alignment, organizational support, IT competencies and organizational awareness of security risks and controls, information security controls can be effectively developed, leading to the success of information security management. Each of these factors affects information security, while the complex solutions include combinations of all of them.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2019 Volume 6 Number 4 (June)
http://doi.org/10.9770/jesi.2019.6.4(37)

Zamman and Razali (2016) identified three aspects of information security management success factors based on expert opinions – people, process and organization. Waly, Tassabehji and Kamala (2012) concluded that information security can be managed through three separate mechanisms: organizational factors, behavioral factors and education.

In the paper by Kazemi et al. (2012), the authors identified the following factors for the success of the implementation of information security management: support for senior management, information security policy, labor responsibility, employee motivation, awareness and training programs, information security compliance, international standards, and the use of information security services by external consultants.

Alnatheera (2015) identified the following factors of successful information security management - promoting top management for information security, creating an effective information security policy, information security and training and organizational culture. Alnatheera (2015) also stated that ethical norms and policies may vary from country to country.

Based on the previous literature review we have decided to narrow down the scope of our research and focus on 4 main factors of success of information security management, defined by most of the authors as the most important: *Compliance of information security management with the company's business activities (F1), Support of top management (F2), Security controls (F3) and Organizational awareness (F4)*. All factors are also expressed in the ISO 27001 standard.

Focus on the *factor F1* can be defined as follows. Business compliance and business strategy with information security management strategy are consistency in addressing needs, requirements, goals, and information security management structures. An effective strategy must ensure and protect information assets while enabling business. Experts have pointed out that protecting information resources from potential threats should be part of a business strategy as it can provide a competitive advantage to a business (Soomro et al., 2016). Information security objectives and activities must be consistent with business objectives and requirements and be managed by business management (Kayworth and Whitten, 2010; Ma et al., 2009). There must be close collaboration between information security managers and business managers.

Information security management practices must be consistent with the organization's business strategies (Chang et al., 2011). The aim of reconciling information security with the business strategy is to support business objectives in the business sector (Herath et al., 2010). Security management must be business-driven and based on business goals, values or needs (Spears and Barki, 2010).

The role of the *second factor F2* may be justified by the following findings of the experts in the field. Soomro et al. (2016) emphasize the role of management in information security management. Management must actively support information security efforts at all levels. Top management engagement can in many ways support information security - from funding and human resource allocation to highlighting the importance of security for other business components (Kayworth and Whitten, 2010).

Kazemi et al. (2012) consider supporting top management as an important factor in the success of information security management. Whitman and Mattord (2012) argue that providing information security is the responsibility of the top management. Promoting top management is very important for successful information security management (Kayworth and Whitten, 2010; Ma et al., 2009; Ma et al. 2009; Tu and Yuan (2014). In addition, top management plays the most important role in creating effective organizational structures, as organizational structure is very important to information security management.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2019 Volume 6 Number 4 (June)
http://doi.org/10.9770/jesi.2019.6.4(37)

The role of the *factor F3* refers to technical and procedural information security controls, including risk management, security policies and application of standards. Organizations need to implement security controls and use them to protect information security. Security policies and countermeasures can protect information systems from security risks. Tu, et al. and (2018). Tu and Yuan (2014) identified the following crucial processes for developing security controls: *risk management, security policy implementation, and compliance*. Risk management is considered the most effective approach to identifying the most effective set of security controls. Security policies are an example of organizational solutions to security problems - they are countermeasures and strategies taken to reduce systemic risks. If an enterprise wants to successfully implement information security management, the relevant standards must be followed (Yildirim et al., 2011).

The factor F4 refers to workers' knowledge of information security risks, policies and related practices. In a broader sense, this also includes an information security culture, that is the way in which people rely on information security in the enterprise. Employees should have adequate literacy in case of information technology. IT literacy provides the basis for key security concepts (Culnan et al., 2008). Waly, Tassabehji and Kamala (2012) emphasize the need for education. Thus, training can increase employee awareness, understanding and participation in information protection (Ma et al., 2009). It is of the utmost importance that the company supports standards and procedures for building information security, says Tu and Yuan (2014). Information security policy will not be effective without training (Soomro et al., 2016). Empirical evidence suggests that it is difficult to implement security controls if people do not have sufficient training on best IT security practices (Werlinger et al., 2009).

3. Aim and methodology

The aim of this paper is to identify the factors of success of information security management in segment of SMEs. The research is geographically focused on Slovakia. At the base of the literature research of the most important information security management success factors the research team narrowed the scope of the research at four main factors: *Compliance of information security management with the company's business activities (F1), Support of top management (F2), Security controls (F3) and Organizational awareness (F4).*

The research team formulated the following scientific hypotheses:

H1: Four main factors (F1 to F4) of information security management are equally important.

H2: The cause and effect relationship among the factors of information security management (F1, F2, F3 and F4) does not exist.

In small organizations, responsibility for safety management is concentrated at the level of the statutory body, as it is not effective to employ a dedicated full-time security manager. Another solution is to accumulate functions within an enterprise or outsource an information security manager (CISO). The questionnaire research in the field of information security management of SMEs is quite problematic. Kotulic and Clark (2004) conducted a survey related to information security management in the USA and found that as many as 23 percent of the respondents who refused to answer the questions in the questionnaire declared that they are not eager to share any information about their computer security policies with outside entities.

Facing the risk of getting unreliable data from not sufficiently experienced respondents the research team decided to conduct the research with the use of the structured expert evaluation method applied on a selected group of senior IT security experts accompanied by the use of appropriated sophisticated statistical tools. We have

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2019 Volume 6 Number 4 (June)
http://doi.org/10.9770/jesi.2019.6.4(37)

addressed ten senior information security management experts from the insurance and banking sectors in Slovakia and asked them to respond to our questions. None of the contacted experts refused to cooperate. This number of experts is sufficient for the method of structured expert evaluation since the usual number of experts for the DEMATEL technique is around six – the quantity if replaced by the quality and preciseness in this case (Lo and Chen, 2012, Tianshui and Gang, 2014, Hu and Chen, 2016). The questions in the survey were formulated in a way that allowed to evaluate the answers using the DEMATEL technique. The experts evaluated the significance of four factors from the view point of success of information security management. When making expert estimates, the experts were asked to address the issue of information security management in a specific area, namely in case of SMEs. The results of the expert evaluation were processed using the DEMATEL technique.

The DEMATEL technique (Decision making trial and evaluation laboratory) is considered to be an effective method for identifying the components of the cause and effect chain of a complex system. This technique deals with evaluating interdependent relationships between factors and identifying critical factors through a structural model with the use of a digraph to illustrate relationships.

Lo and Chen (2012) proposed a hybrid procedure for assessing the level of information security in various security controls using the DEMATEL technique. Tianshui and Gang (2014) have proposed a new security and privacy assessment model for the information system. Hu and Chen (2016) identify important security factors for e-government cloud computing using DEMATEL.

DEMATEL was developed at the Geneva Research Center at the Battelle Memorial Institute (Tan and Kuo, 2014).

While considering the number of n factors F_1, F_2, ..., F_n. in a first step the experts E_1, E_2, ..., E_m are invited to quantify the direct effect of factor F_i on factor F_j $(i,j = 1,2,\dots,4; i \neq j)$. The experts evaluate the significance of factors using the "no impact (0)", "low impact (1)", "medium impact (2)" "high impact (3)" and "very high impact (4)" scales.

We designed individual direct-influence matrices from the expert evaluations. By aggregating expert opinions, we got a group direct-influence matrix:

$$Z = (z_{ij}); z_{ij} = \frac{1}{m}\sum_{k=1}^{m} z_{ij}^{k} \;;\; i,j = 1,2,\dots,n.$$

The normalized direct-influence matrix is obtained using the following transformation:

$$X = \frac{1}{s} Z;\; s = \max\left\{\max_{1\le i\le n}\sum_{j=1}^{n} z_{ij},\; \max_{1\le j\le n}\sum_{i=1}^{n} z_{ij}\right\}.$$

Using the normalized matrix of direct influence, we calculated the total influence matrix T = (t_{ij}) by adding all the direct effects and all indirect effects

$$T = X + X^2 + \cdots + X^h = X(I - X)^{-1}, \text{ for } h \to \infty,$$

where I is a unit matrix.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2019 Volume 6 Number 4 (June)
http://doi.org/10.9770/jesi.2019.6.4(37)

In the next step, we constructed an influential relation map (IRM). Let R be the vector of the sums of the individual columns and C is the vector of the sums of the individual columns of the matrix T. Then

$$R = (r_i) = \left(\sum_{j=1}^{n} t_{ij}\right); i = 1, \dots, n$$

and

$$C = (c_j) = \left(\sum_{i=1}^{n} t_{ij}\right); j = 1, \dots, n.$$

Values r_i ; $i = 1, \dots, n$, represent the sum of the direct and indirect effects that depend on factor F_i towards other factors.

Values c_j; $j = 1, \dots, n$ represent the sum of the direct and indirect effects that factor F_j receives from other factors.

Values $r_i + c_i$; $i = 1, \dots, n$ represents degree of central role. The higher the centrality degree is, the more important the factor is.

Values $r_i - c_i$; $i = 1, \dots, n$ shows the degree of relation. Relation divide the criteria in to cause and effect group. If $r_i - c_i$ is positive then factor F_i belongs to cause group. If $r_i - c_i$ is negative then factor F_i belongs to effect group.

The representation of the values (R + C, R-C) in the graph gives us valuable information for the decision making. Factors in quadrant I are identified as major factors. They have a high degree of importance and important relationships. Factors in quadrant II are identified as driving factors because they are of little importance but a high degree of relationships. Factors in quadrant III have little importance and little degree of relationships. They are relatively disconnected from the system. Factors in quadrant IV are of high importance, and low degree of relationships; so-called impact factors. They are influenced by other factors. They cannot be directly improved.

In many articles there is a threshold value used. It allows to filter out negligible effects. We determined the threshold value as the maximum value of the diagonal elements of the matrix *T* (Tan and Kuo, 2014).

We calculate the weight of importance of the i - th criterion from the relationship

$$w_i = \frac{r_i + c_i}{\sum_{i=1}^{n}(r_i + c_i)}; i = 1, 2, \dots, n.$$

4. Results and Discussion

The following matrices present the results of the DEMATEL technique application. A group direct-influence matrix *Z*, normalized group direct-influence matrix *X* and total influence matrix T are as follows

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2019 Volume 6 Number 4 (June)
http://doi.org/10.9770/jesi.2019.6.4(37)

$$Z = \begin{pmatrix} 0 & 3.1 & 1.9 & 3.2 \\ 3.6 & 0 & 3.9 & 3.8 \\ 2.9 & 3.0 & 0 & 3.6 \\ 2.2 & 2.0 & 3.3 & 0 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 0.27 & 0.17 & 0.28 \\ 0.32 & 0 & 0.35 & 0.34 \\ 0.26 & 0.27 & 0 & 0.32 \\ 0.19 & 0.18 & 0.29 & 0 \end{pmatrix},$$

$$T = \begin{pmatrix} 0.75 & 0.92 & 0.94 & 1.10 \\ 1.21 & 0.91 & 1.27 & 1.39 \\ 1.04 & 1.00 & 0.88 & 1.23 \\ 0.86 & 0.81 & 0.96 & 0.82 \end{pmatrix}.$$

The threshold value 0.91 was chosen as the maximum value of the diagonal of the total influence matrix *T*.

Table 1. Total relation matrix and the causal influence levels

	F1	F2	F3	F4	R	C+R	R-C
F1	0	0,92	0,94	1,1	2,96	5,21	0,71
F2	1,21	0	1,27	1,39	3,87	5,79	1,94
F3	1,04	1	0	1,23	3,27	6,44	0,12
F4	0	0	0,96	0	0,96	4,68	-2,77
C	2,25	1,92	3,17	3,72			

Source: Own calculations

Note: F1 – Compliance; F2 - Top Management; F3 - Security Controls; F4 – Awareness.

The importance of the four factors is prioritized based on $(r + c)$ values. It is evident from Table 1 that the most important factor within the causal relation is F3 (Security Controls) with the largest $(r + c)$ value 6,44 and factor F2 (Top Management) with the $(r + c)$ of 5,79, followed by the F1 (Compliance) with the value of 5,21. The factor F4 (Awareness) is a little less important with the value of 4,68. *The hypothesis H1 was rejected* – the importance of the selected factors F1 to F4 is not equal. In case of the limited budget on information security management, SME should focus the attention on the *Security controls* at the first place.

The centrality degree represents the strength of the effect on success of information security management. The results of the research identified that the *Security Controls* is the most important factor of success of information security management. The results of technical and procedural information security controls, risk management and application of standards reflect the success of information security management. The second most important factor is the *supportive top management*. Top management really plays the most important role in the company in the field of information security. This result is in line with the articles that highlight the importance of top-management support. Information security management must be consistent with the company's business activities. They must not prevent them but help them. Therefore, the importance of the compliance with information security management with business activities of the company is considered as relevant. Several studies have also confirmed the importance of organizational awareness.

The weight of the factors corresponds with significance is presented in the Figure 1.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2019 Volume 6 Number 4 (June)
http://doi.org/10.9770/jesi.2019.6.4(37)

Figure 1. The weight of the factors
Source: Own calculations

Based on the (r-c) values, the specified four factors were divided into the cause group (4) and the effect group (1). The positive value of (r-c) of the factor classified it to the cause group that directly affected the others. The highest (r-c) valued factors also had the greatest direct impact on the others. The factors F2 (1,94), F1 (0,71) and F3 (0,12) belong to cause group in our case study.

The negative value of the (r-c) of the factor meant that this factor is largely influenced by the others and classified it to the effect group. In case of our research the factor F4 was categorized in the effect group, with the (r-c) value equal to -2,7. *Organizational awareness (F4)* was the affected the most by *Compliance of information security management with the company's business activities (F1), Support of top management (F2), Security controls (F3)*. These results allow us to reject the *hypothesis H2* – factors F1, F2 and F3 do affect the factor F1.

From the total relation matrix *T* we will construct an impact-relation map for the success of information security management.

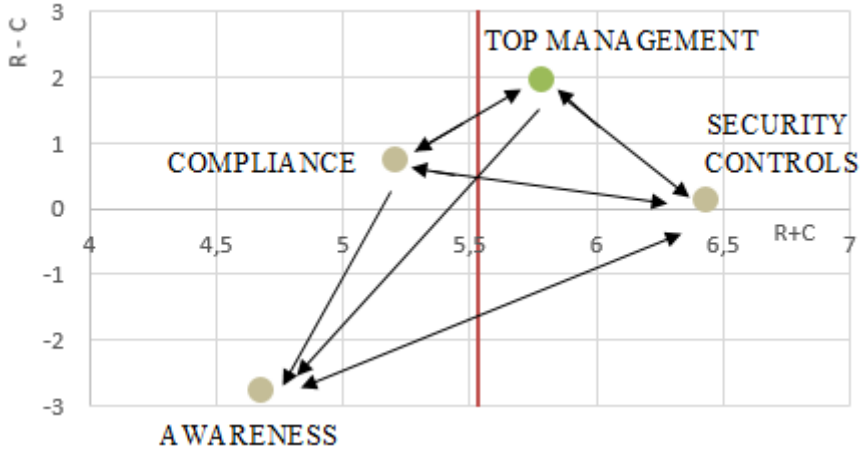

Figure 1. The cause and effect diagram (Influential relation map IRM)
Source: Own calculations

The reasoning factors, that are affecting the others, are the most fundamental. These factors not only promote the information security management directly, but also influence the other factors. They are the key factors to establish the long-effect mechanism of the successful security management system. The importance of the top management of the company can hardly be under evaluated since the top management directly influences all the processes inside the company. In spite of the fact, that the factor F2 (the supportive top management) was

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2019 Volume 6 Number 4 (June)
http://doi.org/10.9770/jesi.2019.6.4(37)

identified as the second most important factor, our results also confirmed that the influence of this factor on the other ones is the highest. The effect of the other two factors – compliance of information security management with business activities of the company and security controls – is weaker, but still significant. Any pair of the three factors *Compliance of information security management with the company's business activities (F1), Support of top management (F2), Security controls (F3)* are mutually influenced by each other.

The result factors are the most direct factors to promote the information security management in the company, but they can be easy influenced by the other factors. Due to this fact our results imply that the factor of organizational awareness (F4) is the most obvious and important factor for the success of information security management in the short term.

Supportive top management especially in area of education, training, increasing IT literacy skills will certainly help the success of management of information security. Compliance of information security management with business activities of the company will also support employees' interest in increasing IT skills. Higher IT skills allow workers to achieve better results in their workplace. Compliance with security policies, standards reduce systemic risks.

The issue of information security management becomes vitally important, especially in the segment of small and medium sized enterprises. The basic reason why SMEs become a popular target for cyber-attacks is the fact that attackers are usually looking for simple goals. Small companies with limited budgets often do not consider cyber security to be important, are easier to disrupt than large ones that invest large amounts in the security of information systems (Millaire et al. 2017).

While 77% of cybercrime focuses on SMEs, 58% of SME managers do not consider cyber-attacks to be a significant risk and 65% of SMEs do not have a security policy, only 10% of computer crimes reported to the police by small and medium-sized enterprises result in the conviction of offenders (FireEye, 2016).

Conclusions

The issue of information security management becomes vitally important, especially in the segment of small and medium sized enterprises. The aim of this paper was to identify the factors of success of information security management in segment of SMEs in Slovakia.

Based on the previous literature review we have narrowed the scope of our research and focused on 4 main factors of success of information security management, defined by most of the authors as the most important, which were *Compliance of information security management with the company's business activities, Support of top management, Security controls and Organizational awareness*. To identify the importance and interconnections of the specified factors we have addressed senior IT security experts from small and medium sized enterprises in Slovakia. The experts evaluated the significance of four factors from view point of success of information security management and the results of the expert evaluation were processed using the DEMATEL technique.

The results of the research show that the *Security Controls*, including technical and procedural information security controls, risk management and application of standards reflect the success of information security management is the most important factor of success of information security management. The second most important factor is the *supportive top management*. Our results also imply that the factor of organizational awareness is the most obvious and important factor for the success of information security management *in the short-term* period.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2019 Volume 6 Number 4 (June)
http://doi.org/10.9770/jesi.2019.6.4(37)

Our results imply that SMEs should promote organizational awareness in information security management in line with implementation of the security controls at the first line of the defense in order to protect the information, as the most valuable asset of the company.

Our research has some limitations, mostly related to the number of the experts involved, that was explained by the general unwillingness of the SMEs representatives to share the data about the information security management in their companies. The impact of this limitation was reduced by the usage of the DEMATEL technique, so the results are statistically representative.

References

ADÁSKOVÁ, P. (2009). Ekonomická krize zvyšuje zájem firem o řízení rizik. Risk-Management.cz, ISSN 1802-0496.

ALNATHEER, M. A. 2015. Information security culture critical success factors. In: *12th International Conference on Information Technology-New Generations – Proceedings,* 2015. s.731-735

Badulescu, D. (2012). SMEs financing: The Extend of Need and the Responses of Different Credit Structures. Theoretical and Applied Economics, 17(7), pp. 25-36

Belás J., Macháček J., Bartoš P., Hlawiczka R., Hudáková M. (2014). Business Risks and the Level of Entrepreneurial Optimism among SME in the Czech and Slovak Republic. Journal of Competitiveness, 6(2), pp. 30-41.

BHAIRD, C.M. (2010). Resourcing Small And Medium Sized Enterprises. Springer Verlag: Berlin, 2010.

CULNAN, M. J., FOXMAN, E. R., RAY, A. W. 2008. Why It Executives Should Help Employees Secure Their Home Computers*, In: MIS Quarterly*, 2008. *ISSN* 0276-7783, roč. 7, č. 1, s. 49-56

DAVIDAVIČIENĖ, V., RAUDELIŪNIENĖ, J., TVARONAVIČIENĖ, M., KAUŠINIS, J**.** 2019**.** The importance of security aspects in consumer preferences in electronic environment. Journal of Security and Sustainability Issues*,* 8(3), 399-411. http://doi.org/10.9770/jssi.2019.8.3(9)

DAVIDEKOVA, M., GREGUS ML., M., FARKAS, P. 2016. MATLAB implementation of the recent CCC construction approach. *International conference on telecommunications and signal processing*, TSP 2016, pp. 429-432. https://doi.org/10.1109/tsp.2016.7760913

DEKÝŠ, P. 2010. Správa informačnej bezpečnosti v malej a stredne veľkej spoločnosti *e-Focus*, 2010. ISSN 1336-1805, roč. 10, č. 3, s. 12-13

Fire Eye, Inc.. 2016. 5 reasons cyber attackers target SMEs, FireEye, 2016. [cit. 2018-10-11] Available at: https://www.fireeye.com/content/dam/fireeye-www/global/en/offers/pdfs/SMEInfographic_web.pdf

GRÓDEK-SZOSTAK, Z. NESTERAK, J., 2017. Trade missions as the instrument for supporting international technological cooperation of enterprises - Case study of Poland, Slovakia and Czech Republic. Acta Oeconomica Universitatis Selye 6 (2), 57 – 68. ISSN 1338-6581

HAU B., PENROSE M., HALL T., BEVILACQUA M. 2016. *M-Trends, 2016*. EMEA Edition, Jún, 2016

HENDERSON, J., WEILER, S. (2010). Entrepreneurs and Job Growth: Probing The Boundaries Of Time And Space, Economic Development Quarterly, 24(1), 23 – 32.

HUANG, S., M., LEE, C. L., KAO, A.C. 2006. "Balancing Performance Measures for Information Security Management: A Balanced Scorecard Framework," In: *Industrial Management and Data Systems,* 2006. ISSN 0263-5577, roč. 106, č. 2, s. 242-255

HUDEC, L. 2014. *Manažment informačnej bezpečnosti - csirt.sk* [cit. 2018-10-11] Available at: https://www.csirt.gov.sk/doc/MFSRVzdelavanie/02Vzdelavanie2014/Prezentacie_vyssi_manazment_organizacie/PrezGR_Manazment_IB.pdf

CHANG, S. E., CHEN, S.Y., AND CHEN, C.Y. 2011. Exploring the Relationships between It Capabilities and Information Security Management In: *International Journal of Technology Management*, 2011. ISSN 0267-5730, roč. 54, č. 2/3, s.147- 166

CHMIELARZ W., ZBOROWSKI M. 2017. Analysis of the Use of Electronic Banking and e-Payments from the Point of View of a Client, 2017, In: *Proceedings of the Federated Conference on Computer Science and Information Systems*, 2017. s. 965-969, [cit. 2018-05-10].

KARPAK, B., & TOPCU, I. (2010). Small medium manufacturing enterprices in Turkey: an analytic network process framework for prioritizing factors affecting success. International Journal of Production Economics, 125, pp. 60–70.

KAYWORTH, T., WHITTEN, D. 2010. Effective Information Security Requires a Balance of Social and Technology Factors, In*: MIS Quarterly Executive*, 2010. ISSN 1540-1960, roč.9, č, 3, s.163-175

KAZEMI, M., KHAJOUEI, H., NASRABADI, H. 2012. Evaluation of information security management system success factors: Case study of Municipal organization. In: *African Journal of Business Management*, 2012, roč. 6, č. 14, s. 4982-4989. ISSN 1993-8233

KHOURI, S. 2009. Analýza bezpečnosti informačných systémov organizácií. In *Zborník z UNINFOS 2009 (Univerzitné informačné systémy),* 2009. Slovenská poľnohospodárska univerzita v Nitre. 2009, s. 140-144, ISBN 978-80-552-0309-6

KORENKOVA, V., ZAVADSKY, J. LIS, M. 2019. Linking a performance management system and competencies: qualitative research. *Engineering management in production and services*, Vol. 11, No. 1, pp. 51-67. DOI: 10.2478/emj-2019-0004

KOTULIC, A. G., CLARK, J. G. 2004. Why there aren't more information security research studies. *Information & Management*, roč. *41, č.*5, s. 597-607.

LENGYEL, P., OLÁH, J., PANCSIRA, J., FÜZESI, I., POPP, J. 2017. Advantages of using LMS in training for agricultural advisors. *Acta Oeconomica Universitatis Selye* 6(2), 109 – 118. ISSN 1338-6581

LO, C. C., CHEN, W. J. 2012. A hybrid information security risk assessment procedure considering interdependences between controls. In: *Expert Systems with Applications*, 2012. ISSN 0957-4174, roč. 39, č., s. 247-257

LOPES, I., OLIVEIRA, P. 2015. Implementation of information systems security policies: a survey in small and medium sized enterprises. In: *New Contributions in Information Systems and Technologies, Volume 1,* 2015. s. 459 - 468, ISBN 978-3-319-16486-1

MA, Q., SCHMIDT, M. B., PEARSON, J. M. 2009. An Integrated Framework for Information Security Management, In: *Review of Business*, 2009. ISSN 2378-9670, roč. 30, č. 1, s. 58-69

MACIEJEWSKI, M., WACH, K. 2019. International Startups from Poland: Born Global or Born Regional? *Journal of Management and Business Administration. Central Europe*, 27(1), 60-83. https://doi.org/10.7206/jmba.ce.2450-7814.247

MANDORF, S., GREGUS, M. 2014. The e-business perspective as a solution for inertia against complexity management in SME. *Proceedings - 2014 International conference on intelligent networking and collaborative systems, IEEE INCOS 2014*, pp. 237-241

MILLAIRE P., SATHE A., THIELEN P. 2017. What All Cyber Criminals Know: Small & Midsize Businesses With Little or No Cybersecurity Are Ideal Targets, 2017. [cit. 2018-10-11] Available at: https://www2.chubb.com/usen/_assets/doc/17010201-cyber-for-small_midsize-businesses-10.17.pdf

OLAH, J., KOVACS, S., VIRGLEROVA, Z., LAKNER, Z., KOVACOVA, M., POPP. J. 2019. Analysis and comparison of economic and financial risk sources in SMEs of the Visegrad Group and Serbia. *Sustainability*, Vol. 11, No. 7, 1853. https://doi.org/10.3390/su11071853

PERACEK, T., MITTELMAN, A., MUCHA, B. 2018. The Particular Aspects of Procurement Contracts of Trading in Securities in the Conditions of the Slovak Republic. *Finance and sustainability*. *Springer Proceedings in Business and Economics*, pp. 175-185. https://doi.org/10.1007/978-3-319-92228-7_15

POLKOWSKI, Z., DYSARZ, J. 2017. IT Security management in small and medium enterprises. In*: Scientific Bulletin – Economic Sciences*, 2017. ISSN 1583-1809, roč. 16, Special Issue EtaEc, s. 134-148

RADU, L. D. 2018. Green ICT: some challenges and potential solutions. *Acta Oeconomica Universitatis Selye* 7 (2), 141 – 150. ISSN 1338-6581

RAJNOHA, R., KORAUŠ, A., & DOBROVIČ, J. (2017). Information systems for sustainable performance of organizations. Journal of Security and Sustainability Issues, 7(1), 167-179. https://doi.org/10.9770/jssi.2017.6.1(14)

SKLENÁR, D., ČIMOVÁ, K. 2018. *IKT v MSP*. In: Acta Paneuropeana - Letters in economics and international business. 2018. roč. 2, ISBN 9788089453399

Slovak Business Agency. (2015). Správa o stave MSP v SR 2014. Available at: http://www.sbagency.sk/sites/default/files/sprava_o_stave_msp2014.pdf

SOOMRO, Z.A., SHAH, M.H., AHMED, J. 2016. Information security management needs more holistic approach: a literature review, In: *International Journal of Information Management*, ISSN 0268-4012, roč. 36, č. 2, s. 215-225

SPEARS, J. L., AND BARKI, H. 2010. User Participation in Information Systems Security Risk Management. In: *MIS quarterly,* 2010. ISSN 2162-9730, roč. 30, č. 3, s. 503-522

TAN, W.K., KUO, C. Y. 2014. Prioritization of facilitation strategies of park and recreation agencies through DEMATEL analysis. In: Asia Pacific Journal of Tourism Research. 2014. ISSN XXXX, roč. 19, č. 8, s. 859–875

TIANSHUI, W., GANG, Z. 2014. A new security and privacy risk assessment model for information system considering influence relation of risk elements. In: *2014 Ninth International Conference on Broadband and Wireless Computing, Communication and Applications IEEE*, 2014, s. 233-238. ISBN 978-1-4673-8315-8

TU, Z., YUAN, Y. 2014. Critical success factors analysis on effective information security management: A literature review. In: *Twentieth Americas Conference on Information Systems*, Savannah, 2014. s. 1-12. ISBN 978-1-6326-6753-3

TU, C. Z., YUAN, Y., ARCHER, N., CONNELLY, C. E. 2018. Strategic value alignment for information security management: a critical success factor analysis. In: *Information & Computer Security*, 2018. ISSN 2056-4961, roč. 26, č.2, s.150-170

TVARONAVIČIENĖ M. 2018. Towards internationally tuned approach towards critical infrastructure protection, *Journal of Security and Sustainability Issues,* 8(2), 143-150. https://doi.org/10.9770/jssi.2018.8.2(2)

VERBANO, C. AND VENTURINI, K. (2013). Managing risks in SMEs: a literature review and research agenda. Journal of Technology Management & Innovation, 8(3), pp. 186–197.

VILCEKOVA, L., MUCHA, B., PERACEK, T., STRAZOVSKA, L. 2018. Selected issues of family business in selected countries with emphasis on the Slovak republic. *Innovation management and education excellence through Vision 2020, Vols IV -VI,* pp. 2500-2509

WALY, N., TASSABEHJI, R., KAMALA, M. 2012. Improving organisational information security management: The impact of training and awareness. In: *2012 IEEE 14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems,* Liverpool, UK. 2012. s. 1270-1275, ISBN 978-0-7695-4749-7

WERLINGER, R., HAWKEY, K. , BEZNOSOV, K. 2009. "An integrated view of human, organizational, and technological challenges of it security management", In: *Information Management & Computer Security*, 2009. ISSN #0968-5227, roč. 17, č. 1, s. 4-19

WHITMAN, M. E., MATTORD, H. J. 2012. Introduction to information security. In: *Principles of Information Security*, 2012. s. 1-35. ISBN 978-1-111-13821-9

YILDIRIM, E. Y., AKALP, G., AYTAC, S., BAYRAM, N. 2011. Factors Influencing Information Security Management in Small-and Medium-Sized Enterprises: A Case Study from Turkey. In: *International Journal of Information Management*, 2011. ISSN 0268-4012, roč. 31, č. 4, s. 360-365

ZAMMANI, M., RAZALI, R. 2016. An empirical study of information security management success factors. In: *International Journal on Advanced Science, Engineering and Information Technology*, 2016. ISSN 2088-5334, roč. 6, č. 6, s. 904-913

ZAVADSKA, Z., ZAVADSKY, J. 2018. Quality managers and their future technological expectations related to Industry 4.0. *Total Quality Management and Business Excellence*, pp. 1-25. https://doi.org/10.1080/14783363.2018.1444474

ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2019 Volume 6 Number 4 (June)
http://doi.org/10.9770/jesi.2019.6.4(37)

Aleksandr KLJUČNIKOV is an Associate Professor at the University of Entrepreneurship and Law, who deals with the area of the sharing economy, financial and information management, financial and credit risks, corporate and international finance and international trade with the focus on SMEs. He is an author co-author of 3 scientific monographs, 4 chapters in the scientific monographs, more than 60 scientific articles in the per-reviewed journals with over a hundred citations listed at the Web of Science and Scopus databases. At present, he is involved as a solver of five national and internal scientific projects funded by the state and private organisations.
ORCID ID: https://orcid.org/0000-0003-0350-2658

Ladislav MURA is an Associate Professor, a Slovak expert on small and medium business, international business, and the human resource of management. He is the author of 3 domestic scientific monographs on the internationalization of business, small and medium enterprises, human resource management, co-author of foreign scientific monographs. He has published a lot of articles in various scientific journals.
ORCID ID: https://orcid.org/0000-0002-2453-8740

David SKLENÁR is a PhD. Candidate of the Faculty of Economics and Business of Pan-European University in Bratislava, Slovakia.
ORCID ID: https://orcid.org/0000-0001-7358-7453