Agris on-line Papers in Economics and Informatics

Volume VIII Number 4, 2016

Factors Affecting Information Security Focused on SME and Agricultural Enterprises

V. Bolek[1], A. Látečková[2], A. Romanová[1], F. Korček[1]

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

[2] Department of Accountancy, Faculty of Economics and Management, Slovak University of Agriculture in Nitra, Nitra, Slovak Republic

Abstract

Progress in the field of information and communication technology is a source of advantage that improves quality of business services; increases productivity levels and brings competitive advantage to enterprises and organisations related to agricultural production. However, the use of information and communication technology (ICT) is connected with information security risks that threaten business continuity and information assets. The ICT in small and medium-sized enterprises (SME) and agricultural enterprises is the source of several advantages as well as the risks resulting from information security violation and security incidents. This paper aims at the current situation of information security in SME and agricultural enterprises. Furthermore, the paper provides results of a survey focusing on identification and evaluation of the effects of internal and external factors affecting existence of risks in information security in Slovak SME and agricultural enterprises. Until now, there had not been a similar survey carried out.

Keywords

Information security, security incident, risk, factors, SME, agricultural enterprises.

Bolek, V., Látečková, A., Romanová, A. and Korček, F. (2016) “Factors Affecting Information Security Focused on SME and Agricultural Enterprises", *AGRIS on-line Papers in Economics and Informatics*, Vol. 8, No. 4, pp. 37 - 50. ISSN 1804-1930, DOI 10.7160/aol.2016.080404.

Introduction

Significance of ICT has been growing exponentially for the last few years. The need for ICT is unquestionable as it improves quality of services and productivity levels in organisations and businesses in various sectors including agriculture. Investments in information technology have become a dominant part of capital allocation for many organisations. The use of ICT is a source of advantage for organisations and businesses, as well as risk of information security breaches and security incidents. The objective of this paper is to present results of a research studying the effects of selected factors (internal and external) affecting the existence of information security risks and security incidents in small and medium-sized enterprises (SME) and agricultural enterprises in the Slovak Republic (SR), and a comparison with other studies researching the issue.

Nowadays, the issue is of great importance in the agricultural enterprises. These enterprises more often implement mobile technologies, smart devices, GPS trackers, etc. The use of mobile devices in the agricultural enterprises is growing in all countries of the world. Importance and relevance of implementation of the mobile devices and applications were pointed out in the studies of Qiang (2011) and Stočes et al. (2015). The mobile technologies are different from personal computers in their connectivity in particular, which is the most important contribution to the agricultural enterprises. The mobile devices are increasingly becoming vulnerable to possible infiltrations and security breaches. Therefore, the information security issue relates to such devices as well.

Information security has been discussed since the origin of the first computers. Nowadays, it concerts each country, the discussion has become international. The worldwide importance of information security and data protection is growing in parallel with increasing number of attacks and security incidents. Security policies of organisations are not innovated in accordance with technological progress because predicting

further development remains difficult. Theoretical background presents a comparison of academic and professional perceptions of the information security terms and defines the factors used in the survey conducted in Slovak SME.

Information security

Information security, which has become a crucial component of good corporate governance, is a discipline responsible for protecting organisations' information assets against business risks (von Solms and von Solms, 2005). The family of standards ISO/IEC 27000 (2014) considers information security as a preservation of confidentiality, integrity and availability of information. Moreover, additional properties, such as authenticity, non-repudiation, accountability and reliability may also be involved. From a different perspective, information security is the process of protecting information and information infrastructure from unauthorized access that results in disclosure, modification or destruction of information, and modification or disruption of IT services (Ng et al., 2014). The process of information security requires constant attention (Hochmann et al., 2011). Previously, information security issues were treated by technological solutions (Singh et al., 2013). However, growing security needs have extended organisations' attention to explore the management role in information security (Soomro et al., 2016; Siponen et al., 2014; Singh et al., 2013). According to Albrechtsen and Hovden (2010) a performance of information security is based on knowledge and behaviour of various ICT users.

A single or a series of unwanted or unexpected information security events is called an information security incident (ISO/IEC 27000, 2014). An incident is a violation or imminent threat of violation of computer security policies, acceptable use policies or standard security practices (NIST, 2012; Hansman, Hunt, 2005). Therefore, denial of service, unauthorized revelation of sensitive information, a malicious attack on a computing system or network and the unintentional deletion of an important document all qualify as incidents (Ahmad et al., 2015). Many organisations perceive incidents as the activity of a human threat agent (ISACA, 2015). Security incidents are the causes of information security threats in organisations.

A combination of consequences of a security incident and the associated likelihood of occurrence creates an information security risk (ISO/IEC 27005, 2011).

The occurrence of security incidents and information security risks is affected by several external and internal factors. The nature of ICT shows that it is impossible to entirely prevent incidents from occurring. In addition to preventive controls aimed to avoid security incidents, the following elements of incident management are significant – the ability to detect and to evaluate incidents properly, and to implement the appropriate corrective actions (Hochmann et al., 2011). Šindlerová and Butorac (2008) argue that while the importance of risk management has been growing in the process of globalisation, businesses learn to accept risks not just passively, but perceive risks as an opportunity to improve their prosperity. Pačaiová and Markulík (2003) stress that the risk management focuses on ensuring security and stability of a managed system, risk analysis and possible threats. Furthermore, it seeks appropriate corrective and preventive controls to minimise negative impacts of security events and their overgrowth to danger or crisis. It is a process of risk identification, analysis, evaluation and definition of the optimal treatment in order to minimise losses and maximise opportunities (Pačaiová and Markulík, 2003; Tichý, 2006, Kračmár, 2012). Kračmár (2012) understands the optimal treatment as dealing with risks at minimal management costs while respecting business objectives. The following section examines the importance of internal and external factors affecting information security risks in Slovak enterprises.

Factors affecting information security risks

Risk management represents the basis for information security management. It is necessary to meaningfully and effectively manage information security without knowing the risks to confront. Regular risk analysis updates enable to adjust information security strategy when necessary. According to Hamranová (2013), Business Intelligence applications are also significant in the issue as they assist to map security threats, assets and actions related to elimination of risk. Such applications serve to create a possible simulation of a security policy. The occurrence of individual security risks is affected by several factors as follows.

Internal factors:

Ignorance of employees – lack of employee knowledge in the issue might cause great damage and enable irreversible processes. Hamášová and Gerhátová (2012) emphasize the obligation

of employee trainings which clarify procedures to protect sensitive data from undesirable leaks and explain employees' adherence to a security policy of the organisation. In general, theft, misuse and unauthorised manipulation of information (data) are often directly or indirectly accompanied by employees' ignorance of basic principles related to information security. Even if employees are commonly considered as one of the weakest points in the issue, it is often neglected and requires a special approach. Ignorance may only be removed by a targeted training and education with a cooperation of all stakeholders.

Employee behaviour – behaviour and activities of employees and employers in relation to the safety at work have to be deliberately influenced. Employee behaviour represents a set of trained activities. This is reflected in the thought process and determines human thinking and feeling. "When assessing security, it is necessary to recognise that each system is only as strong as its weakest point. In case of information system security, the weakest point is clearly the user" (Tvrdíková, 2008). Human factor is the weakest element in security systems, especially for unconscious behaviour (CFO, 2013). Employees are threatened by infected e-mails and flash drives, they connect to enterprise servers via public Wi-Fi networks, use the same passwords as in the social media accounts, etc. In such cases, the latest security technology and applications against data leak attacks remain helpless to enterprises. Given that attackers are a step forward, it is crucial to arouse prudent user behaviour in enterprises.

Absence of ICT department – importance of ICT department in various business sectors is diametrical. It is obvious that business management efforts should be focused on connecting information strategy and business strategy. If this objective is met, ICT will be more involved in improving business performance and ICT department with business informatics will grow in importance. ICT will become a key component of entrepreneurship and enterprise. Pour and Voříšek (2007) argue that ICT management must reach a level where the continuity of business is not disturbed, because ICT failures might cause a fatal impact on the enterprise. If the senior management wishes to increase the importance of ICT department, it is appropriate to perceive it as a department of high-priority.

Lack of senior management support – information security risk management should be one of the pillars of enterprise information strategy that is directly linked to a strategic plan and a business strategy. Underestimating the importance of information security by the senior management might cause serious and unrecoverable consequences.

Insufficient technical equipment – scientific and technological progress is constantly raising the level of technical equipment, as well as miniaturisation, smart devices, innovative technologies. Using outdated technology has a negative impact on various economic indicators of enterprises and their performance. The use of obsolete hardware makes business informatics vulnerable to new threats. Therefore, it is insufficient to use modern software without adequate hardware equipment that correctly cooperates with software.

Technology faults (hardware, software) – fault is a characteristic difficult to detect prior to technology implementation and thus an assistance of experts is needed. If there are any doubts about a correct operation of technology, the fault must be immediately eliminated. Technology failure causes serious problems that start a chain reaction.

Insufficient software equipment – software must meet enterprise's requirements. It is not sufficient to own only basic computer programs and update software irregularly. Moreover, redundant software means a risk of information security breaches and security incidents as well.

Absence of internal guidelines and standards – growing significance of ICT indicates that a completely prevented occurrence of security incidents is impossible to achieve. In addition to preventive controls, an important element of information security management is the ability to recognise and evaluate security incidents and to implement appropriate corrective actions. We claim that adherence to guidelines and standards systematically protects information assets and effectively responds to security incidents.

Lack of financial resources dedicated to information security management – lack of funds might directly affect a security level and cause a complete failure of information security. Failure of information security arises as a result of underinvestment in software, hardware and education.

External factors:

Certification – a family of standards ISO/IEC 27000 deals with an information security management system (ISMS) and provides a general

and complete overview of information security risk management for different organisations (enterprises, government agencies, non-profit organisations and others). Organisations choose to establish the ISMS and get certified for many different reasons. Based on the Makatúra's classification (2014), the following reasons are defined: ensuring a market and efforts to comply with legal requirements or a market regulator. ISMS supports the organisations' ability to protect information assets, thus assures that confidentiality, integrity and availability of information is preserved. ISMS is the recognized proactive system of information security management within the organisation.

Legislation – in terms of information security, legislation is a subject of many discussions in various international forums. Slovak legislation is directly affected by documents adopted by the European Union and the NATO. Internationally, multilateral agreements are promoted by institutions such as the OSN, OBSE, resp. OECD. Legislation must take into account: ICT owners' concerns, ICT users' needs and rights of both natural and legal persons whose data is processed by ICT. Legislative requirements are often the most important aspect of organisations paying attention to information security (Hochmann et al., 2011).

Governmental support for information security – need for information security has been realised by national governments and intergovernmental organisations, such as the OECD, NATO, United Nations, Group of Eight and international and European organisations for standardisation, which have created various institutions and institutional arrangements for ensuring the protection of information, e.g. European Agency for Network and Information Security (ENISA), Computer Security Incidents Response Teams (CSIRT), etc., and have determined strategic objectives many of which have already been implemented.

Technological progress – currently, the impact of new ICT on business and society is immense. Progressive technologies are applied in all areas of life and business. Zelená (2005) states that especially for ICT, which has now become a phenomenon, equipments that had been experimentally deployed as large-scale, energy-intensive,unreliable and difficult-to-operate, have become small, friendly, highly reliable and energy-efficient. However, the trend grows together with the information security risk and the number of tools and techniques aimed to disrupt information security. Some people are not able to respond to the progress alone, but proper deployment of ICT can help them overcome this handicap.

Natural disaster risk – natural disasters and accidents represent a permanent threat to life or property by their unpredictability and large-scale consequences. Disasters might cause a physical disruption of technical equipments.

Third-party service delivery failure – service delivery and quality of services agreed in contracts must be ensured, applied and followed by the third party. According to Kaluža (2011), the best way to monitor contract compliance is a communication at all levels of governance. Regular reports of activities, audits, inspection dates and a system of multi-level controls are appropriate communication tools.

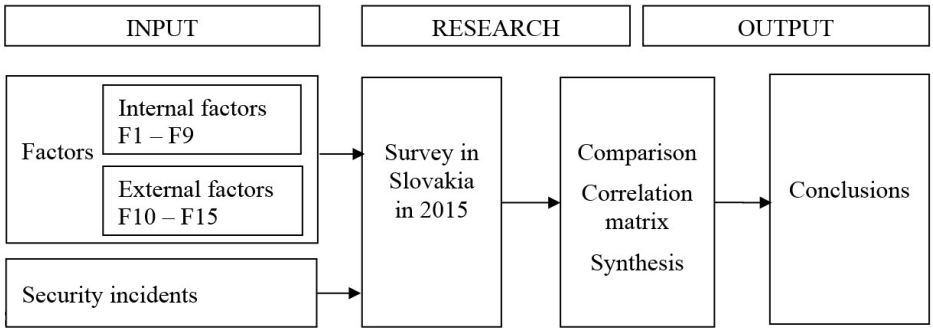
Materials and methods

Based on analysis of theoretical background and conducted surveys in the field of information security, we defined the factors affecting the formation of security incidents and identified that the survey focusing on information security in Slovak SME was missing. In our research, we are more focused on the agricultural enterprises.

Our survey was conducted in 2015. Data were received by an occasional selection of small and medium-sized enterprises in SR segmented by a number of employees. 83 respondents answered the survey in the form of a questionnaire, out of which 20+15 (42.17%) were focused on agricultural production. 20 enterprises were surveyed through the questionnaire and we implemented a structured interview on 15 enterprises.

When designing the questionnaire, valid construct, content and criteria were justified. The questionnaire included open and closed questions. Respondents were asked about their perception of factors that influence the existence of security incidents on a point scale from 0 (insignificant) to 7 (very significant). Research model variables are divided into internal and external factors (Figure 1).

The survey's content and structure are proposed on the basis of the security incidents' current state comparison and the factors affecting the incidents. Data evaluation is performed by using statistical methods, descriptive statistics and the application of quantitative and qualitative statistical methods. Relations between different factors and a formation of security risks are identified by a correlation



Source: own processing

Figure 1: Research model.

analysis at the significance level α = 0.05 and α = 0.01. New information is formulated by comparing the results of the sectional problem areas. A method of comparison serves as a verification tool for theoretical assumptions and survey's results. We use a conceptual approach as the main research method (Balashova et al., 2015).

Moreover, we conducted the structured interviews with managers, identified problems and analysed causes through discussions in the 15 selected agricultural enterprises.

Results and discussion

The concept of security incident can be viewed from multiple angles. However, the nature remains the same. We agree with the definition that a deviation from established rules and standards might lead to information security breaches by the action of security incidents.

More than 20% of enterprises recorded the security incident, which causes the information security breach. Respondents of small enterprises lack a security policy. Only 14% of small businesses implemented the policy.

Security incidents were not experienced by 79.52% of the surveyed enterprises. Out of 35 respondents of the agricultural enterprises, only 2 of them observed security incidents. The high percentage may indicate that the SME do now own the tools to record and assess security incidents or they do not pay much attention to risk management. These results are evidenced by 55.42% of SME which evaluate the information security risks only once a year (this group includes the agricultural enterprises) and 14.46% which do not evaluate the risks at all.

All cases of information security incidents came from external environment. 72% of small enterprises that recorded the security incident indicated the maximum rate (very often) of the emergence of security incidents in their business.

The objective of our survey is to analyse the significance of individual security incidents that concerns the researched enterprises (Table 1).

Enterprises attach the greatest importance to unauthorized penetration into ERP (Enterprise Resource Planning system), M = 5.92, SD = 1.49, and to unauthorized modification of sensitive information, M = 5.90, SD = 1.41. Business information assets (e.g. business secrets, knowledge, financial and management data, personal information, etc.) are crucial to create added value for the business. Theft or any change of such assets might lead to loss of credibility, business know-how and competitiveness. The most important data is stored in ERP systems. For this reason, the greatest threat to businesses is the security incident directed to the business information system. All of the presented security incidents are considered significant by the respondents as they exceed the average value of significance, M = 3.5. Unavailability of ICT services has the lowest mean score M = 4.82, SD = 1.88, but it belongs to significant security incidents as well. Positions of security incidents' concerns are similar considering the agricultural enterprises. Based on the structured interviews, the enterprises indicated that they fear the internet banking penetration and the ERP violation due to ignorance of their employees. Most business processes depend on continuous operation of ICT services. Otherwise productivity decreases, unforeseen downtime arises and normal operation of the business fails. Results of enterprises' risk likelihood perception are shown in Table 2.

Several factors affect the occurrence, respectively the emergence of information security risks. We inquired respondents about their perception

Security incident	N	Min	Max	Mean	Std. Deviation
Malware	83	0.00	7.00	5.1807	1.92001
Botnet	83	1.00	7.00	5.8795	1.53335
Unwanted content (defacement, spam..)	83	2.00	7.00	5.4458	1.84294
Techniques of obtaining information (phishing, social engineering...)	83	0.00	7.00	5.3253	1.96375
Asset vulnerability	83	1.00	7.00	5.0361	1.90280
Unauthorised modification	83	2.00	7.00	5.9036	1.41089
Unavailability of ICT services (DoS, DDoS...)	83	1.00	7.00	4.8193	1.87503
Attempt to penetrate ICT	83	1.00	7.00	5.1446	1.71174
Unauthorised penetration into ERP	83	1.00	7.00	5.9157	1.49148

Note: 0 (insignificant) – 7 (very significant) scale
Source: Authors´ own

Table 1: Significance of security incidents.

Information security risk	N	Min	Max	Mean	Std. Deviation
Disclosure of confidential data	83	0.00	6.00	2.0964	1.74338
Disclosure of business secrets	83	0.00	6.00	2.0120	1.72141
Enterprise brand damage	83	0.00	7.00	3.2651	2.04274
Loss, destruction or damage of personal data	83	1.00	6.00	2.6386	1.92910
Unavailability of ICT services (e-mail, internet, remote access, cloud, website...)	83	1.00	6.00	2.5783	1.38916
Interruption of employee performance	83	0.00	6.00	2.2892	1.82483
Interruption of business operation	83	0.00	6.00	1.6386	1.68623
Hardware failure	83	1.00	4.00	2.7229	1.15096
ERP failure	83	0.00	4.00	1.9277	1.23746
Specialised software failure	83	0.00	4.00	1.9639	1.12017
Office software failure	83	0.00	5.00	2.3133	1.58443
Security system failure	83	0.00	4.00	1.8554	1.27960
Theft of enterprise ICT	83	1.00	5.00	2.1928	1.47713
Power outage	83	1.00	7.00	3.8193	1.64646
Natural disaster (flood, fire, lightning,...)	83	0.00	4.00	1.8313	1.05714

Note: 0 (insignificant) – 7 (very significant) scale
Source: Authors´ own

Table 2: Perception of risk likelihood

of the effect of selected factors on the emergence of information security risks. Internal and external factors of the research model were subjected to statistical research. Partial results of descriptive statistics are presented in Table 3.

Respondents consider the technological progress as the most significant factor, M = 3.98, SD = 2.11. Technological progress in ICT changes the structure of not only economy, but also a number of business areas. It has a significant impact on the lives of individuals and shapes society. The current state of technological progress is resolute. It has great potential, facilitates business management and enriches the lives of individuals. However, there are lots of risks that create opportunities for the emergence of security incidents.

Employee behaviour is the most significant internal factor, M = 3.93, SD = 2.28. In the field of information security, employee education and raising their awareness traditionally produces disinterest, resp. meeting the legal requirements. However, targeted training and education are beneficial in terms of increasing the level of employee information literacy and knowledge of various threats. According to several surveys, most security incidents emerge from ignorance of employees. The only effective control is a comprehensive staff training program.

The third most significant factor is the third-party

Factors		N	Min	Max	Mean	Std. Dev.	Rank
Internal	F1 - Ignorance of employees	83	0.00	7.00	3.3012	1.85929	5.
	F2 - Employee behaviour	83	0.00	7.00	3.9277	2.28347	2.
	F3 - Absence of ICT department	83	0.00	6.00	2.3855	1.69527	13.
	F4 - Lack of senior management support	83	0.00	6.00	2.1566	1.82451	15.
	F5 - Insufficient technical equipment	83	0.00	6.00	3.1325	2.51712	7.
	F6 - Technology faults	83	0.00	7.00	3.2048	2.66302	6.
	F7 - Insufficient software equipment	83	0.00	6.00	3.5181	2.05629	4.
	F8 - Absence of internal guidelines and standards	83	0.00	6.00	2.4096	1.95708	12.
	F9 - Lack of financial resources dedicated to ISMS	83	0.00	7.00	2.2169	1.80817	14.
External	F10 - Certification	83	0.00	7.00	2.5422	1.98961	10.
	F11 - Legislation	83	0.00	5.00	2.7590	1.58184	9.
	F12 - Governmental support for information security	83	0.00	7.00	2.4699	2.13757	11.
	F13 - Technological progress	83	0.00	7.00	3.9759	2.10676	1.
	F14 - Natural disaster risk	83	0.00	7.00	2.9398	1.88931	8.
	F15 - Third-party service delivery failure	83	1.00	7.00	3.8675	2.12862	3.

Note: 0 (insignificant) – 7 (very significant) scale
Source: Authors´ own

Table 3: Factors affecting the emergence of security risks.

service delivery failure, M = 3.87, SD = 2.13. Failure of third-party deliveries might bring irreversible consequences. Enterprises often cannot reverse the process. Therefore, it is important to ensure appropriate and accurate selection of the business partner before any contract is concluded.

The technological progress is the most important factor when analysing the results of the survey conducted in agricultural enterprises. These enterprises do not often have enough financial resources to implement new software applications and modernise hardware equipment to protect enterprises' confidential information, know-how or personal data. Another serious factor is ignorance, respectively the low level of workers' information literacy. It is usual to observe the absence of specific trainings focusing on the use of ICT and the information security.

In addition to respondents' perception of security risk likelihood, we examined the correlation and significance of various factors and information security risk (Table 4).

We conclude that the correlation between internal factors and the security risk is significant at the significance level $\alpha = 0.05$ for F8 - Absence of internal guidelines and standards, $p = 0.022$. The correlation is significant for factors F3 - Absence of ICT department, $p = 0.007$, and F4 - Lack of senior management support, $p < 0.000$, at the significance level $\alpha = 0.01$. Absence of internal guidelines and standards increases the risk of the incident occurrence. Enterprises that do not comply with the guidelines or have not implemented any of them are unable to systematically and adequately protect information assets and effectively prevent security incidents. Proper implementation of the guidelines, standards and policies should be a priority for the senior management. ICT department having sufficiently qualified personnel is responsible to deal with information security management. Absence of the ICT department in the enterprise increases a possibility of the information security risk. Eventually, the senior management that does not support information security risk management creates a space for the emergence of risks and security incidents. If the management underestimates the importance of information security, serious, possibly unrecoverable consequences are caused. Therefore, it is crucial to perceive the information security management as a fundamental pillar of the information strategy, which is a part of the business strategy.

When examining the correlation of external factors and the emergence of security risk, we identified a significant effect of factors F10 - Certification, $p = 0.026$, F12 - Governmental support for information security, $p = 0.034$, and F13

Factors		Information security risk		N
		Pearson Correlation	Sig. (2-tailed)	
Internal	F1 - Ignorance of employees	-0.031	0.780	83
	F2 - Employee behaviour	-0.08	0.472	83
	F3 - Absence of ICT department	0.293**	0.007	83
	F4 - Lack of senior management support	0.438**	0.000	83
	F5 - Insufficient technical equipment	0.082	0.464	83
	F6 - Technology faults	-0.024	0.832	83
	F7 - Insufficient software equipment	0.059	0.597	83
	F8 - Absence of internal guidelines and standards	0.251*	0.022	83
	F9 - Lack of financial resources dedicated to ISMS	0.141	0.203	83
External	F10 - Certification	0.245*	0.026	83
	F11 - Legislation	0.149	0.180	83
	F12 - Governmental support for information security	0.233*	0.034	83
	F13 - Technological progress	0.221*	0.044	83
	F14 - Natural disaster risk	0.004	0.971	83
	F15 - Third-party service delivery failure	0.334**	0.002	83

Note: * Correlation is significant at the 0.01 level (2-tailed).
** Correlation is significant at the 0.05 level (2-tailed).
Source: Authors´ own

Table 4: Correlation of factor effects and the emergence of security risk.

- Technological progress, $p = 0.044$, at the significance level $\alpha = 0.05$. Effect of the factor F15 - Third-party service delivery failure on the emergence of security risk is significant at the significance level $\alpha = 0.01$.

Summary of findings and discussion

EY's (2015) Global Information Security Survey was conducted between June 2015 and September 2015. Participants included 1755 respondents from 67 countries and across all major industries. Compared with 2014-2015, the top two vulnerabilities are:

- Careless or uninformed employees
- Outdated information security controls or architecture

In 2014 these same two vulnerabilities were perceived to be high priorities, but the degree of vulnerability organisations feel has decreased in these areas. Today, only 44% feel vulnerable in relation to uninformed employees, compared with 57% in 2014; only 34% feel vulnerable due to outdated systems, compared with 52% in 2014. This shows that organisations believe they are covering their vulnerabilities more effectively. However, when we look at the top two threats today:

- Phishing
- Malware

These threats ranked 5th and 7th in 2014, with the theft of financial information, the threat of fraud, espionage and zero-day attacks all seen ranked higher.

The survey of Eurostat (2011) shows the state of information security in 27 countries of the European Union. The share of large enterprises that had a formally defined ICT security policy was three times more than the share of small ones. The highest proportion of enterprises having such a policy (52%) in the EU-27 was reported within the sector Information and Communication activities. The lowest proportions, less than one quarter of enterprises, were registered in the sectors Transportation and Storage, Construction and Accommodation and Food Service activities. In January 2010, the highest proportions of enterprises having a formally defined ICT security policy with a plan for regular review were registered in Sweden and Norway (both 46%) followed by Denmark (43%). In more than half of the countries, Information and Communication activities had the highest percentage of enterprises with an ICT security policy. The lowest percentage for enterprises

with such a policy was reported in Accommodation and Food Service activities in a majority of the countries. Less than 10% of the enterprises in Romania, Hungary and Bulgaria reported that they had a formally defined ICT security policy. Another survey will be carried out in 2016. In 2009, the incidents most commonly reported by enterprises were those resulting in unavailability of ICT services, destruction or corruption of data due to hardware or software failures, with shares above 20% registered in Cyprus, Portugal and Finland (26% of enterprises respectively), Denmark (24%), Greece (23%), the Czech Republic (22%) and Slovakia (20%). The highest proportion of enterprises reporting ICT incidents resulting in the destruction or corruption of data due to malicious software infection or unauthorised access was registered in Slovakia (16%), Portugal (14%), Spain (11%) and Greece (10%). The share of enterprises reporting unavailability of ICT services due to an attack from outside was highest in Slovakia (11%) and the Netherlands (7%). In the majority of EU countries, the disclosure of confidential data due to intrusion, pharming or phishing attacks was reported by 1%.

The last information security survey in SR was conducted in 2011 (Hochmann et al., 2011). The survey covered 180 respondents. Decline in the share of enterprises, that recorded the existence of a security incident, from 55% in 2009 to 37% in 2011, is considered as a positive finding. The most common security incidents are malware (43%), software failure (38%), power outage (14%), hardware failure (12%) and network connectivity failure (8%). Other security incidents, such as user error, theft of equipments, information leaks, external attacks, misuse of devices and user password disclosure, occur less frequently (5%).

In each survey, the significance of individual security incidents is assessed. However, the structure and perception are different because of the scope of each survey. Table 5 compares the order of incidents' significance in conducted surveys (E&Y, 2015; Eurostat, 2011; Hochmann et al., 2011).

A specific survey focusing on the analysis of factors affecting the existence of security incidents was found absent. Not only in relation to SME, but also focusing on the enterprises engaged in agricultural production. This fact resulted in implementation of a new survey. The significance of individual factors perceived by SME is presented in the results. The current state of significant factors affecting

Security incidents	RANK			
	Ernst&Young 2015	Eurostat 2011	MF SR 2011	Own research 2015
Destruction of hardware		1	4	6
Destruction of software			2	
Data destruction	4			
Malicious software	2	2	1	5
Unauthorised access	3	2		4
Loss of confidential data	4	3	7	6
Unavailability of ICT services due to external attacks		1		7
Botnet				2
Unauthorised modification				1
Attempt to penetrate enterprise ICT	6		8	5
Power outage			3	
Network connection failure			5	
Internal attacks (user error)	6	2	6	
Natural disasters	6			
Spam	6			3
Fraud	5		7	
Zero-day attacks	2			
Phishing	1	3	10	4
Theft of financial information	3			

Source: E&Y, 2015; Eurostat, 2011; Hochmann et al., 2011

Table 5: Significance of security incidents – a comparison of surveys.

the existence of security incidents in Slovak enterprises is influenced by the current state abroad due to open economy. Enterprises undertake numerous measures to comply with standards, guidelines and security policies while their interest in certification is growing. Observance of standards and policies reduces the likelihood of security risks. However, certification is not mandatory as organisations might meet the requirements and objectives of information security management without any need to possess the ISMS certificate. Studying recent findings of the International Organisation for Standardisation's survey that counted certified organisations in accordance with the ISO/IEC 27001 standard in 2014, it is possible to observe an increase in the number of certified organisations by 7% (+1623) compared to 2013. The world total is 23972 issued certificates according to the above standard. In SR, 162 certificates were distributed, which represented an increase of 3 units over the previous year. The top countries are Japan (7181), Great Britain (2261), India (2170) and China (2002) (ISO, 2014).

We identified that governmental support for information security is significant. Therefore, national information security strategies define strategic goals, recommendations and measures to meet the requirements. The Slovak national strategy forms a general framework for information security in the country by its distribution of power and competencies, priority setting and proposals towards achieving the objectives. The actual support is represented by the formation of legislation and standards. According to the National strategy for information security in SR, which was approved in 2008, information security remains multilateral. In SR, a coordinator of information security and the area of classified information is the Ministry of Finance, which is preparing a law dedicated to information security management in organisations. This law will mainly consolidate the requirements, competencies and responsibilities regarding the security of ICT. The proposal of the information security law is designed in accordance with the ICT development; it reflects changes in the public administration and self-governing bodies and takes the guidelines and recommendations of the European Union into account. Currently, the National Security Authority of the Slovak Republic submitted an action plan to the Slovak Government. The action plan includes controls, activities and authorities responsible for their implementation, which should reduce the risk of cyber attacks. The proposed controls create conditions for an integrated, coordinated and effective system for the protection of Slovak cyberspace. The whole process should be concluded by the year 2020. Preparation and presentation of the information and cyber security law proposal commences in 2016. The fact that the protection of cyberspace is not explicitly and comprehensively regulated in the Slovak law is considered to be the most serious problem in this area in SR.

Technological progress is the important external factor not only in Slovakia. Outdated enterprises' hardware and software provide opportunities for new threats, and thus increase the security risk. Monitoring possible third-party service delivery failure and communication failure is under the responsibility of inspection team. Any failure does not immediately introduce a security incident, but creates space for the risk and the likelihood of its existence.

Security incidents that arise in the internal environment occur mainly due to lack of education and training. Managers and other employees must be educated in the issue and must be instructed in a secure ICT usage. Targeted training should be a standard component of security controls in the enterprise. According to Eurostat (2011), the highest share of trainings focused on information security is carried out in Cyprus (77%) and Finland (74%). Hochmann (2011) claims that training contributes to building security awareness and helps to prevent faults. Training in information security is appropriate, desirable and currently evolving (Bishop, 2000). If enterprises are not sufficiently aware of the need for information security, it is necessary to create legal requirements as this aspect is often the only motive of enterprises to deal with information security. According to Hochmann (2011), a problem arises within affected organisations that primarily try to fulfil obligations (e.g. development of a security project, guidelines) with the objective of avoiding penalties. The quality of these documents and the real effort to increase the level of information security usually remains of secondary importance. After demanding elaboration of information security documents enterprises rarely undergo the information systems audit and update the documents regularly. Information security management and risk management should be seen as the essential and continuous process of providing competitive advantage in the current business environment. The ICT has a significant impact on increasing competitiveness of the agricultural enterprises and the enterprises engaged in agritourism (Havlíček et al., 2009).

They have the competitive advantage and offer the possibility to make themselves visible in the market, strengthen their market position and attract new customers. Maumbe (2010) and Vaněk (2011), also point to the ICT as a powerful tool of the competitiveness in agriculture and rural development as well as in developing countries.

Based on the survey conducted in the selected agricultural enterprises, we can conclude that the number of employees decreases in recent years and the management positions are being accumulated. In most of the surveyed enterprises, a separate organisational unit for the ICT governance was not created. Moreover, it is confirmed in our analysis that the absence of the separate unit has a significant impact on the creation of security incidents. Even if the ICT is available for employees, they often have to cope with only basic ICT knowledge. This means that at the lower levels of management, the low level of knowledge in the issue is observed. It is followed by the behaviour of the employees which is characterised by lax approach towards the information security (employees not paying sufficient attention to ensuring the basic data security, i.e. passwords are either not defined, or one password is shared by several workers). Nowadays, the level of completed trainings and courses aimed at increasing the level of managers' information literacy is very low.

The management of the agricultural enterprises often underestimates the information security risks and relies on the basic security controls, e.g. antivirus programs. At the same time, there is insufficient technical equipment (outdated technology). On the other hand, we confirm that the software applications are updated on a regular basis. We could not find a single enterprise without having updated its economic or antivirus software. Undoubtedly, the small and medium-sized agricultural enterprises lacked an internal directive for the ICT management and administration. According to our research, the main reasons for the shortcomings is the missing financial resources.

Conclusion

After the evaluation of the survey, a downward trend of security incidents compared to the previous period can be observed. 20% of respondents admitted that security incidents are considered satisfactory. Taking into account the current state of the agricultural enterprises, we conclude that it is necessary for managers to address the information security issues. The key area is human resources and the availability of skilled IT personnel. Increasing the educational level in information security is desirable. The results of external and internal factors' effects indicate that compliance of governmental support and legislation continues to be a major driving force in the information security improvement. Senior management that supports the active information security management and the existence of ICT department generates opportunities to improve the competitive advantage. The use of consistent procedures, rules, policies, regulations, guidelines, certification and other supporting tools ensures permanent and adequate level of enterprise information security and eliminates the security risk existence. However, the continuous technological progress brings rapid changes, therefore all stakeholders must continually educate in order to be able to identify new threats and incorporate controls into the implemented strategy of information security.

We were able to identify and evaluate the current state of information security in Slovak SME with respect to the agricultural enterprises and the effects of factors affecting information security risk existence by the conducted survey. It is possible to reduce or increase the occurrence of security incidents by influencing the areas linked to the factors.

Acknowledgements

The knowledge presented in the paper was obtained as a result of the Grant VEGA 1/0489/15, Increasing the efficiency of decision making by managers with the support of information systems and accounting.

Corresponding author:
Ing. Vladimír Bolek, PhD.
Department of Information Management, Faculty of Business Management
University of Economics in Bratislava, Dolnozemská cesta 1, 852 35 Bratislava, Slovak Republic
Phone: +421 2 6729 5622, E-mail: vladimir.bolek@euba.sk
ORCID: 0000-0003-1144-278X

References

[1] Ahmad, A., Maynard, S. B. and Shanks, G. (2015) "A case analysis of information systems and security incident responses", *International Journal of Information Management*, Vol. 35, No. 6, pp. 717 – 723. ISSN 0268-4012. DOI 10.1016/j.ijinfomgt.2015.08.001.

[2] Albrechtsen, E. and Hovden, J. (2010) "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study", *Computers & Security*, Vol. 29, No. 4, pp. 432 – 445. ISSN 0167-4048. DOI 10.1016/j.cose.2009.12.005.

[3] Balashova, N. N., Šilerová and E., Melikhov, V. A. (2015) "Developing the metodology to form integrated reporting of agroholdings in the Russian Federation", *AGRIS on-line Papers in Economics and Informatics*, Vol. 7, No. 4, pp. 19 - 29. ISSN 1804-1930.

[4] Bishop, M. (2000) "Education in information security", *Concurrency*, IEEE, Vol. 8, No. 4, pp. 4 -8. ISSN 1092-3063. DOI 10.1109/4434.895087.

[5] Butoracová Šindlerová, I. and Butorac, D. (2008) "Aplikácia krízového manažmentu na malom a strednom podniku zaostávajúceho regiónu s primárnym zameraní na význam ľudských zdrojov v organizácii", *Collection of papers of scientific papers of department of economy and economics ANNO* (in Slovak), University Prešov, Prešov. ISBN 978-80-8068-798-4.

[6] Ernst & Young. (2015) "*Global Information Security Surey 2015*", Ernst & Young, [Online]. Available: http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf [Accessed: 10 Jan. 2016].

[7] Eurostat (2011) "*ICT security in enterprises 2011*". [Online]. Available: http://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_security_in_enterprises [Accessed: 20 Dec. 2015].

[8] CFO (2013) "*Ako hackeri klamú vašich zamestnancov"* (in Slovak), CFO. [Online]. Available: http://www.cfo.sk/articles/ako-hackeriklamu-vasich-zamestnancov [Accessed: 20. Dec. 2015].

[9] Hamášová, K. and Gerhátová, G. (2012) "Návrh systému vzdelávania v oblasti informačnej bezpečnosti v podniku agrosektora" , *Collection of network and information technology 2012* (in Slovak). [Online], Slovak University of Agricultural in Nitra. Available: http://spu.fem.uniag.sk/konferencie_a_seminare/sit/2012/zbornik/hamasova_gerhatova.pdf [Accessed: 20. Dec. 2015].

[10] Hamranová, A. (2013) "Aspekty implementácie Business Intelligence v slovenských podnikoch", *Ekonóm*, ISBN 978-80-225-3603-5.

[11] Hansman, S. and Hunt, R. (2005) "A taxonomy of networks and computer attacks", *Computers & Security*, Vol. 24, No. 1, p. 31–43. ISSN 0167-4048. DOI 10.1016/j.cose.2004.06.011.

[12] Hochmann, J., Stanek, M., Vazan, I. (2011) "*Prieskum stavu informačnej bezpečnosti vo verejnej správe v Slovenskej republike 2011*", Ministry of Finances of the Slovak Republic. [Online]. Available: http://www.informatizacia.sk/ext_dok-prieskum_ib_2013_-sk-en-/16943c [Accessed: 15 Dec. 2015].

[13] Havlíček, Z., Lohr, V., and Benda, P. (2009) "ICT and agritourism in Czech Republic", *APSTRACT: Applied Studies in Agribusiness and Commerce*, Vol. 3, [Online]. Available: http://ageconsearch.umn.edu/bitstream/53541/2/10_ICT_Apstract.pdf [Accessed: 12 Jan. 2016].

[14] ISACA (2015) "*Cybersecurity Fundamentals Study Guide*", ISACA, ISBN 978-1-60420-593-0.

[15] ISO (2014) "*ISO Survey*", International Organization for Standardization. [Online]. Available: http://www.iso.org/iso/home/standards/certification/isosurvey.htm? certificate= ISO/IEC% 2027001&countrycode =AF#standardpick [Accessed: 8 Jan. 2016].

[16] ISO/IEC 27000:2014. Information technology – Security techniques – Information security management systems – Overview and vocabulary

[17] ISO/IEC 27005:2011. Information technology – Security techniques – Information security risk management.

[18] Kaluža, F. (2011) "Outsourcing z pohľadu riadenia informačnej bezpečnosti", *International magazine for security engineering*, Vol. 6, pp. 1-2. ISSN 1336-9717.

[19] Kračmár, J. (2012) "*Riadenie operačných rizík v krízovom riadení podniku*", Krízový manažment podniku. ISBN 978-80-225-3520-5.

[20] Makatúra, I. (2014) "*Čo je to bezpečnostný počítačový incident?*", ITNews, [Online]. Available: http://www.itnews.sk/2014-11-24/c166583-co-je-to-bezpecnostny-pocitacovy-incident [Accessed: 21 Dec. 2015].

[21] Maumbe, B. M. and Okello, J. (2010) "Uses of Information and Communication Technology (ICT) in Agriculture and Rural Development in Sub-Saharan Africa: Experiences from South Africa and Kenya", *International Journal of ICT Research and Development in Africa (IJICTRDA)*, Vol. 1, No. 1, pp. 1-22. DOI 10.4018/jictrda.2010010101.

[22] Ng, Z. X., Ahmad, A. and Maynard, S. B. (2014) "Information security management: Factors that influence security investments in SMES", *Proceedings of the 11th Australian Information Security Management Conference*, [Online], Available: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1156&context=ism [Accessed: 9 Jan. 2016].

[23] NIST (2012) "*Computer Security Incident Handling Guide*", National Institute of Standards and Technology, U.S. Department of Commerce, Aug. 2012, [Online], Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf [Accessed: 9 Jan. 2016].

[24] Qiang, C. Z., Kuek, S. C., Dymond, A., Esselaar, S. and Unit, I. S. (2011) "*Mobile applications for agriculture and rural development*", World Bank, Washington, DC.

[25] Pačaiová, H. and Markulík, Š. (2011) "Bezpečnosť technických systémov ako súčasť v zabezpečovaní kvality", *Kvalita*, Vol. 11, No. 11. ISSN 1335-9213

[26] Pour, J. and Voříšek, J. (2007) "Výsledky průzkumu řízení informatických služeb v ČR", *Systémová integrace*, [Online]. Available: http://www.cssi.cz/cssi/vysledky-pruzkumu-rizeni-informatickych-sluzeb-v-cr [Accessed: 20. Dec. 2015].

[27] Singh, A. N., Picot, A., Kranz, J., Gupta, M.P . and Ojha, A. (2013) "Information security management (ISM) practices: lessons from select cases from India and Germany", *Global Journal of Flexible Systems Management*, Vol. 14, No. 4, pp. 225–239. ISSN 0972-2696. DOI 10.1007/s40171-013-0047-4.

[28] Siponen, M., Mahmood, M. A. and Pahnila, S. (2014) "Employees' adherence to information security policies: an exploratory field study", *Information and Management*, Vol. 51, No. 2, pp. 217 – 224. ISSN 0378-7206.

[29] Soomro, Z. A., Shah, M. H. and Ahmed, J. (2016) "Information security management needs more holistic approach: A literature review", I*nternational Journal of Information Management*, Vol. 36, No. 2, pp. 215 – 225. ISSN 0268-4012. DOI 10.1016/j.ijinfomgt.2015.11.009.

[30] Stočes, P., Vaněk, J., Masner, J., and Jarolímek, J. (2015) "*Mobile application development options for news and information portals*", Future Communication, Information and Computer Science proceedings, CRC Press, Leiden, pp. 111-114. ISBN 978-1-138-02653-7.

[31] Tichý, M. (2006) "Ovládaní rizika", *Analýza a management*, pp. 396. ISBN 80-7179-415-5.

[32] Tvrdíková, M. (2011) "*Aplikace moderních informačních technologií v řízení firmy*", Grada Publishing, pp. 172. ISBN 978-80-247-2728-8.

[33] Vaněk, J., Jarolímek, J., and Vogeltanzová, T. (2011) "Information and Communication Technologies for Regional Development in the Czech Republic-Broadband Connectivity in Rural Areas", *Agris on-line Papers in Economics and Informatics*, Vol. 3, No. 3, pp. 66-76. ISSN 1804-1930.

[34] Von Solms, B. and von Solms, R. (2005) "From information security to…business security?", *Computers & Security*, Vol. 24, No. 4, pp. 271 – 273. ISSN 0167-4048. DOI 10.1016/j.cose.2005.04.004.

[35] Zelená, H. (2005) "*Inovácia a zvýšenie efektivity vzdelávania prostredníctvom IKT*", Preparation of teachers and actual changes in basic education. [Online]. Available: http://www.pf.jcu.cz/structure/departments/kpe/upload/files/konf05-sbornik-22-zelena_h.pdf [Accessed: 28. Dec. 2015].