Agris on-line Papers in Economics and Informatics

Volume XI Number 1, 2019

Data Protection and Security in SMEs under Enterprise Infrastructure

Marcela Hallová[1], Peter Polakovič[1], Edita Šilerová[2], Ivana Slováková[3]

[1] Faculty of Economics and Management, Slovak University of Agriculture in Nitra, Slovak Republic

[2] Faculty of Economics and Management, Czech University of Life Sciences Prague, Czech Republic

[3] The Institute of Foreign Languages, Technical University in Zvolen, Slovak Republic

Abstract

Information is becoming a highly valued commodity of strategic importance in the period of globalization of trade, cooperation and mutual integration of companies. These facts bring a new perspective and the importance of adequate information security in IS/IT, especially in connection with their electronization and electronic exchange. The protection and security of IS/IT is therefore becoming increasingly important for companies and is one of the key factors for the economic success of SMEs, as well as in agricultural organizations and rural development organizations. Management's interest in IS/IT security and information results not only from a threat to prosperity, but also in the case of the threat to the company's own existence. By analysing the risks, adopting IS/IT security policy, developing safety standards, and implementing security in the life of the company, the security process does not end but comes into a qualitatively new stage. At the moment when the main problems are solved and the environment, at least to a certain extent ready, there is time for important routine activities. This is monitoring, control and audit.

Keywords

Security of IS/IT, SMEs, incidents, risks.

Hallová, M., Polakovič, P., Šilerová, E. and Slováková, I. (2019) "Data Protection and Security in SMEs under Enterprise Infrastructure", *AGRIS on-line Papers in Economics and Informatics*, Vol. 11, No. 1, pp. 27-33. ISSN 1804-1930. DOI 10.7160/aol.2019.110103.

Introduction

The deployment of information systems and information technology has become a prerequisite for the success of companies in all areas of economic activity today. IS/IT has been one of the decisive factors for the development and competitiveness of economic organizations in all three sectors (Vaněk et al., 2011; Collins et al., 2006). Without information technology, the work with information is not only inefficient nowadays, but also impossible. In addition, our dependence on these systems is increasing every day. However, the rapid development of modern technologies and information systems is also increasing the possibility of abuse (Leede et al., 2005; Smith, 2003; Kumar et al., 2011). There are a variety of security incidents, such as unauthorized data manipulation (deletion, altering, abusive and consequential misuse), stopping the entire organization from collapsing the infected information system, and others. In addition, today's Internet is constantly rotating other unintended threats looking for any possible deficiency in the security of workstations (Boer et al., 2003). According to Kumar et al. (2011) there is an unprotected PC with Windows operating system after being plugged into the Internet attacked on average within twenty minutes, which is a double increase compared to 2005, when it took about forty minutes. According to several authors Leede et al. (2005); Corso et al. (2001); Hosťovecký et al. (2015); Vaněk et al. (2009), the process of achieving and maintaining confidentiality, integrity, availability, accountability, authenticity, reliability of information and IT services must be at an appropriate level in the current conditions. According to Bresnahan et al. (2002); Zairi et al. (1995); Maglio et al. (2009) protection of information during their creation, processing, storage, transmission and disposal through logical, technical, physical and organizational measures that must counter the loss of confidentiality, integrity and availability of these important business values.

According Wielky (2017); Jones et al. (2003) security management is formulated in the organization on the basis of the following three security policies: the overall security policy of the organization is the set of security principles and regulations that define how to secure the organization as a whole. The IT security organization's overall IT security policy is the managerial view of IT security, it tracks the overall security policy, defines the core strategy, goals, attitudes, roles, responsibilities, and principles related to security-related activities of the IT organization. The overall security policy is the basic information resource for building lower and specific levels of security documentation.

IS security policy has already specifically defined how the overall IT security policy for the particular IS will be adopted and implemented. It contains detailed standards, rules, practices and regulations specifically defining how to manage, protect and distribute sensitive information and other IT resources within the organization and the particular IS (Erumban et al., 2006). The principles of IS security policy elaboration are formulated on the basis of specified requirements in the field of computer security, system security requirements of the given IS in the documents of the overall IT security policy, the results of IS risk analysis, safety requirements stated in laws, regulations, standards, regulations and standards (Šimek et al., 2008). In the literature, the concepts of the overall IT security policy and IS security policy often blend under the unified name of security policy, or system security policy (McAdam, 2006).

According to Leach (2008), it is typical of most companies that meet the goal definition: The goal is to eliminate potential direct and indirect losses due to misuse, damage, destruction, or unavailability of information by creating a comprehensive, cost-optimized and efficiently functioning information security management system.

Three basic rules defining safety objectives in the IS (Jai Arul et al., 2011) are as follows:

- ensuring confidentiality and integrity,
- ensuring the availability of information and information system services,
- ensuring the responsibility of the user of the information system for his / her activity therein.

If the effort is to make the system a chance for success, it is imperative to convince the leadership of the necessity and the usefulness of this step. IS / IT security does not just mean the purchase of HW and SW, this process requires the development of the set of internal directives and regulations that must be respected and strictly observed. As always, in the IS / IT industry, the most common challenge in introducing changes is the attitude of regular users whose thinking needs to change (Manas-Argemi, 2005). Management support is therefore a key prerequisite for project success. It is precisely because of the lack of this support that many security projects, regardless of their quality, will end up with the initial design of the paper or at a different stage of elaboration with the only effect, with the unnecessary means and forces of IS security staff. According to Miller (2012), the implementation of safety measures does not generate any immediate direct profit for the organization - on the contrary, investment in its deployment and maintenance is not negligible. However, in the event of extraordinary events, it becomes invaluable.

The main importance of security policy is prevention. In the long run, it is nowadays a necessary part of the overall security policy of the organization. Security policy protects business investment (hardware & software & know-how). IS/IT security certificates increase corporate credibility - a competitive advantage with today's insignificant meaning. At the same time, the security policy prevents damage to the company's reputation by spelling out data leakage by almost eliminating the possibility of leakage. And in case any leakage has yet occurred, the security policy has precise guidelines on how to maintain it and is the argument against accusations of unreliability. Detailed tracking of the entire system blocks illegal activities before damage occurs, or at least immediately detects weaknesses, making it impossible for data to be repeatedly leaked in the same way. Miller (2012) and Hennyeyová et al. (2010) states that the objective of any risk analysis within an organization is to identify and quantify the risks so that they can decide on their acceptability or decide on the adoption of additional measures to reduce them. The magnitude of the risk is determined on the basis of the likelihood of occurrence of the risk and the magnitude of the impact. IS Risk Analysis being a key activity in the security solution process that must provide answers to the following three basic questions: "What happens when information is not protected?", "How can information security be compromised?", "How likely it will become? ". A typical output of the analysis is the document describing the system description and the results of the analysis, i.e. the level of threats, identified vulnerabilities, the level of existing safeguards and the distribution of the resulting risks.

Materials and methods

The aim of our research was to collect material and verify hypotheses that were determined on the basis of theoretical training and knowledge of the current level of solving problem. The main focus of the research was to address the current security threats in enterprises. The aim of this article is to identify and analyse the causes of current IS / IT security incidents and risk factors and their impact on current businesses in terms of creating and improving security policy and protecting sensitive electronic data. The results of our empirical research can serve to concretely improve the security policies of individual businesses, thus avoiding the security threats that current e-times bring. The issue of security of enterprise information systems is currently being addressed by many reputable authors and is considered to be crucial in terms of business operation and competitiveness. The security policy of organizations and compliance with security standards is essential and a key activity leading to the protection of sensitive corporate data of clients and leads to the overall information security of the business itself.

Based on the theoretical knowledge of domestic and foreign literature and practical experience from our previous publications, we have decided to determine the following hypotheses of our empirical research.

H1: The security of a business information system of a particular organization depends to a large extent on compliance with the established security policy of the organization and the compliance with established safety standards of the enterprise.

H2: The human factor and ignorance of safety standards of technology security management is the biggest threat of loss and aft of data in an enterprise.

The benchmark sample consisted of 36 medium -sized enterprises in Slovak republic. The questionnaire contained a total of up to 25 questions that were specifically targeted to the area of enterprise information system security and the main stakeholders were IS/IT security managers and IS/IT administrators as well. Data collection was conducted through a questionnaire survey, which was composed of the groups that were assigned to individual questions. The questionnaire was constructed from closed questions for better clarity and evaluation. Reliability of the questionnaire was performed using Cronbach's alpha. The variables in the position of static and dynamic parts of the hypothesis were compared by Kuskal-Wallis to use more than two variables.

$$\alpha = (k/(k-1)) * (1 - \Sigma s^2_i / s^2_{sum})$$

k - number of items

s^2_i - variance for k items

s^2_{sum} - variance for the sum of items

Hypothesis was tested by standard statistical methods, hypothesis testing was performed by the Kruskal-Wallis test, which is an extension of the Mann-Whitney U test to use more than two variables. Analyses of the attribute group show that the reliability of the data obtained from the main survey is sufficient (internal consistency of the scale is considered appropriate even if the coefficient is greater than 0,7). The values are given in Table 1.

Range of reliability analysis	Number of items surveyed	Value of Cronbach’s alpha
All variable items	15	0.862
Hypothesis H1 variables	7	0.891
Hypothesis H2 variables	8	0.846

Source: own research and processing

Table 1: Overview of the introduction and use of management methods and techniques.

Results and discussion

In empirical research, we mainly focused on whether businesses are interested in the current state of their IS/IT security in the enterprise, and whether businesses are interested in monitoring their security technologies. Practical experience from our survey has produced results that we can generalize as follows. A major challenge is the enforcement of standards and methodologies of IS/IT security from the theoretical to practical level. We can safely say that support for top management in IS/IT security is low, says 81% of respondents. Likewise, 71% of respondents claim that the interest in IS/IT security in an organization is manifested mainly by the security incident itself, and systematic control and updating stagnates. The bottom line, however, is that most of the 91% questioned are aware of security policy and business safety standards, but are aware that employees lack the skills and knowledge they possess. Surprisingly, I'm not willing to find out my current IS/IT security status. Up to 61% of companies are not interested in detecting their current state of information and communications technology security. Part of companies 39%, are interested in finding their actual state of information and communication technology security. We also note that most businesses 90% are not interested in external IS/IT security management, consider it unnecessary and expensive, only 10% would consider external security management collaboration with their systems.

Testing of the H1 hypothesis focused on the assumption that the security of the enterprise information system of a particular organization depends to a large extent on compliance with the established security policy of the organization and the compliance with the established business safety standards. Simple statistical validation can be based on the analysis of the averages from the established security policy values and their comparison with the average of the values with the specified attributes. Same trends of variables would suggest that the hypothesis is valid. Conversely, different trends would suggest that we cannot confirm the hypothesis. The results of this simple comparison are shown in Table 2. Based on the test, we can accept the hypothesis H1.

Range of values	Average
100-71	71.12
70-51	63.23
50-21	42.69
20-0	39.32

Source: own research and processing

Table 2: Results of statistical comparison of mean to H1.

Testing the H2 hypothesis focused on the assumption that the human factor and ignorance of the safety standards of the technological security management is the greatest threat of loss and theft of data in the enterprise. The statistical validation may be based on the analysis of the averages from the detected human factor values and the ignorance of the safety standards and their comparison with the average of the mean values with the specified attributes. Based on the test, we can accept the H2 hypothesis. According to the calculated data, the descending order is evident, but the trends show greater differences than in the hypothesis H1. The comparison results are shown in Table 3.

Range of values	Average
100-71	83.05
70-51	61.17
50-21	46.88
20-0	31.45

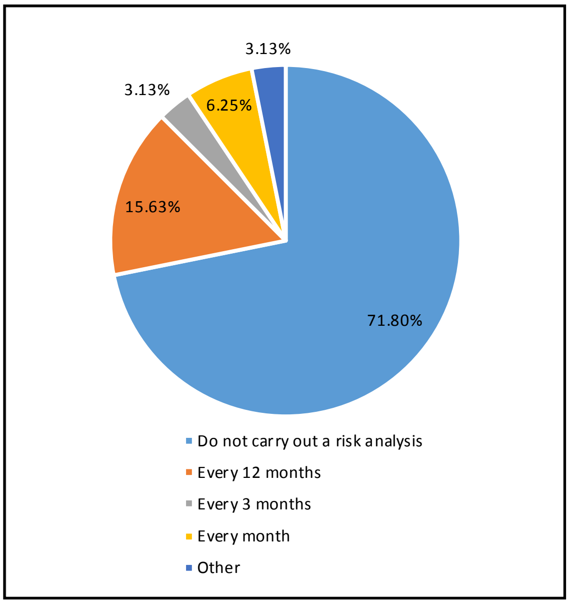
Source: own research and processing

Table 2: Results of statistical comparison of mean to H2.

Our empirical research clearly shows the majority of the 89% questioned that an unambiguous trend in the IT security of information and communication technologies in an enterprise is the application of multi-level and combined IS/IT security protection. The essence of multi-level and combined IS/IT security protection is to deploy more types, types and technological levels of interconnected and cooperative IS/IT security systems. In the absence of identification of the security threat or failure of a certain IS/IT security technology level, another IS/IT security system assumes a different level of detail.

There is no unambiguous solution to eliminate the causes of IS/IT security incidents. In addition, each company is specific in a number of aspects: its field of expertise, staff, technology, IS/IT, etc. It is, however, possible to avoid an adequate combination of process management of IS/IT security and IS/IT security technologies by reducing the risk of security incidents. An important factor in reducing the number of safety incidents is the human factor. Security training and employee training in the sense of the importance of IS/IT security could contribute to the reduction. On the basis of the results obtained, we have confirmed that the human factor affects the security of information and communication technologies at all levels. For users, this is especially the lack of awareness, underestimation of security risks.

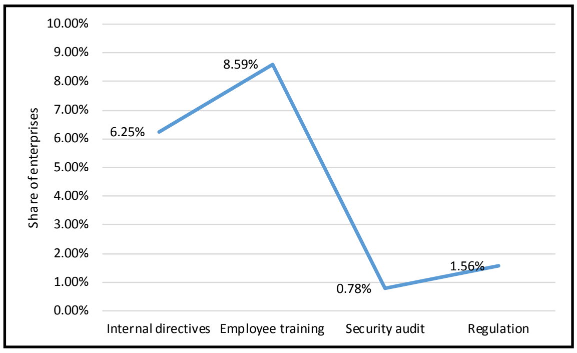
While all subjects provide IS/IT protection, up to 71.88% of these entities do not analyse the potential risks that may be threatening for their IS/IT, as seen in Figure 1.



Source: own research and processing

Figure 1: Performing IS/IT security risk analysis.

We can see the link between the percentage of developed and implemented Security Policy and Security Project documents, because in the preparation of these documents, the subjects would be guided by risk analysis at certain time intervals directly resulting from these documents and audit of IS / IT security. Everything continues, and it is also the case of informing the staff of the subjects about the security and threats to IS/IT, as shown in Figure 2. Only the very lack of security documents causes these low levels of awareness, respectively higher degree of lack of information of employees. However, account must also be taken of the general knowledge of employees and their previous qualifications in this area. Every individual is an ICT user, whether at work or at home. Therefore, it must take care of information security and have minimal knowledge about it if it is just a regular user. An employee should already have this knowledge on the workplace.



Source: own research and processing

Figure 2: Security awareness and threats to ICT.

Conclusion

Information is a highly valued commodity of strategic importance in the period of globalization of trading with a greater degree of cooperation, dynamism and mutual integration of companies. These facts bring a new perspective and importance of adequate information security in IS / IT, especially in connection with their electronization and electronic exchange. The protection and security of IS / IT is therefore becoming increasingly important for companies and is one of the key factors in the company's competitiveness and economic success. The IT security and information is therefore not only a threat to prosperity and competitiveness, but also to the extreme existence of an enterprise. If we compare our empirical research with EY's Global Information Security Survey 2013, we get a very similar match in terms of low-interest companies in the overall security audit once a year, inadequate staff training on IS / IT security. EY's Global Information Security Survey 2013 as well as our unambiguously demonstrates that SMEs have neglected to prevent burglary attacks in the long run and are also not trying to eliminate human factor defects within companies. On farms the situation is similar, data and information are mostly stored on local disks. The computers where the data is stored are on the user's table with any security. Very similar is the situation in companies involved in rural development. Companies have little confidence to outsource corporate security firms and fear the misuse of sensitive corporate data. Despite these reasons, most of the managers interviewed are 81% aware of online-related threats, which we consider to be paradoxical. In spite of the vast amount of IS / IT security issues related to standards, methodologies, security processes, terminology, partial security solutions, IS / IT security manager's profile and status, and a number of documented IS / IT security case studies there are still other and other security threats affecting companies and companies.

Acknowledgements

This article was created with the support ULS in Prague, no. 20181007 – „Geographic data lifecycle with regard to processing automation, application scalability, and adoption of new technologies“.

Corresponding authors
PaedDr. Peter Polakovič, Ph.D.
Department of Informatics, Faculty of Economics and Management
Slovak University of Agriculture, Tr. A. Hlinku 2, Nitra, 949 01, Slovak Republic
Email: darryl.j@manipal.edu

References

[1] Boer, H. and Gertsen, F. (2003) „From continuous improvement to continuous innovation: a (retro)(per)spective”, *International Journal of Technology Management,* Vol. 26, No. 8, pp. 805-827. ISSN 1741-5276. DOI 10.1504/IJTM.2003.003391.

[2] Bresnahan, T., Brynjolfsson, E. and Hitt, L. M. (2002) "Information technology workplace organisation and demand for skilled labour: firm level evidence", *Quarterly Journal of Economics*, Vol. 117, No. 1, pp. 339-76. ISSN 0033-5533. DOI 10.3386/w7136.

[3] Collins, C. J. and Smith, K. G. (2006) "Knowledge exchange and combination: The role of human resource practices in the performance of high technology firms", *Academy of Management Journal*, Vol. 49, No. 3, pp. 544-560. ISSN 1948-0989. DOI 10.5465/amj.2006.21794671.

[4] Corso, M. and Paolucci, E. (2001) "Fostering innovation and knowledge transfer in product development through information technology", *International Journal of Technology Management*, Vol. 22, No. 3, pp. 126-148. ISSN 1741-5276. DOI 10.1504/IJTM.2001.002958.

[5] Erumban, A. A. and Jong, S. B. (2006) "Cross-country differences in ICT adoption: A consequence of Culture?", J*ournal of World Business*, Vol. 41, No. 4, pp. 302-314. ISSN 10909516. DOI 10.1016/j.jwb.2006.08.005.

[6] Hennyeyová, K. and Depeš, P. (2010) "Analysis of the exploitation of information and communication technologies in the agri-food sector companies“, *Agricultural Economics*, Vol. 56, No. 9, pp. 403-408. ISSN 0139-570.

[7] Jai Arul, G., Sanjeev, C. and Suyambulingom, C. (2011) "Implementation of Data Security in Cloud Computing", *International Journal of P2P Network Trends and Technology*, Vol. 1, No. 1. pp. 112-127. ISSN 2249-2615.

[8] Jones, P., Beynon-Davies, P. and Muir, E. (2003) "E-business barriers to growth within the SME sector", *Journal of Systems and Information Technology*, Vol. 7, No. 2, pp. 1-25. ISSN 1328-7265. DOI 10.1108/13287260380000771.

[9] Kumar, V., Batista, L. and Maull, R. (2011) "The Impact of Operations Performance on Customer Loyalty", *Service Science*, Vol. 3, No. 2, pp. 158-171. 2164-3970. DOI 10.1287/serv.3.2.158.

[10] Leach, J. (2008) "Do new information and communications technologies have a role to play in the achievement of education for all?", *British Educational Research Journal*, Vol. 34, No. 6, pp. 783-805. ISSN 1469-3518. DOI 10.1080/01411920802041392.

[11] Leede J. and Looise J. K. (2005) "Innovation and HRM: Towards an integrated framework", *Creativity and Innovation Management*, Vol. 14, No. 2, pp. 108-117. ISSN 1467-8691. DOI 10.1111/j.1467-8691.2005.00331.x.

[12] Maglio, P. P., Vargo, S. L., Caswell, N. and Spohrer, J. (2009) "The service systemis the basic abstraction of the service science", *Information Systems and eBusiness Management*, Vol. 7, No. 4, pp. 395-406. ISSN 1617-9846.

[13] Manas - Argemí, A. (2005) "Security metrics and measurements for IT“, *European Journal for Informatics*, Vol. 13, No. 6, pp. 89-103. ISSN 1684-5285.

[14] McAdam, R. (1996) "An integrated business improvement methodology to refocus business improvement efforts", *Journal of Business Process Re-engineering and Management*, Vol. 2, No. 1, pp. 63-71. ISSN 1355-2503. DOI 10.1108/14637159610111482.

[15] Miller, K. W. (2012) "Security and Privacy Considerations", *IT Professional*, Vol. 14, No. 5., pp. 53–55. ISSN 15209202.

[16] Power, R. (2002) "CSI/FBI computer crime and security survey“, *Computer Security Issues & Trends*, Vol. 8, No. 1, pp.1–24. ISSN 2225-0506.

[17] Smith, M. (2003) "Business process design: correlates of success and failure", *The Quality Management Journal*, Vol. 10, No. 2, pp. 38-49. ISSN 10686967. DOI 10.1080/10686967.2003.11919062.

[18] Šimek, P., Vaněk, J. and Jarolímek, J. (2008) "Information and communication technologies and multifunctional agri-food systems in the Czech Republic Plant", *Soil and Environment*, Vol. 54, No. 12, pp. 547-551. ISSN 2075-1141. DOI 10.17221/426-PSE.

[19] Vaněk, J. Jarolímek, J. and Šimek, P. (2009) “Information Services and ICT Development in Agriculture of the Czech Republic”, *AGRIS on-line Papers in Economics and Informatics*, Vol. 1, No. 1, pp. 47-52. ISSN 1804-1930.

[20] 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. 67-76. ISSN 1804-1930.

[21] Wielky, J. (2017) "The impact of the internet of things concept development on changes in the operations of modern enterprises”, *Polish Journal of Management Studies*, Vol. 15, No. 1, pp. 262-275. ISSN 2081-7452. DOI 10.17512/pjms.2017.15.1.25.

[22] Zairi, M. and Sinclair, D. (1995) "Business process re-engineering and process management”, *Business Process Management Journal*, Vol. 1, No. 1, pp. 161-173. ISSN 1463-7154.