Agris on-line Papers in Economics and Informatics

Volume IX Number 1, 2017

Information Security and Risk Analysis in Companies of Agriresort

M. Hallová[1], P. Polakovič[1], R. Virágh[1], I. Slováková[2]

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

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

Abstract

Information and communication technologies are a tool to streamline production, and therefore they must be properly secured. The article is aimed at solving security and protection of agribusiness ICT. For a more detailed analysis of this issue there has been carried out a research. Its partial results were submitted to statistical analysis and are presented in the following article. The basic prerequisite for the implementation of any safety measures is the risk analysis when properly conducted it enables the effective implementation of safety measures and the corresponding potential threats and protected values of organization. The main aim of this paper is to assess the impact of particular forms of ICTs on protection, determination of the possible impact of the implementation of the risk and threat analysis for the enterprise.

Keywords

Information and communication technologies, information security, security policy, risks, agriculture subject.

Hallová, M., Polakovič, P., Virágh, R. and Slováková, I. (2017) "Information Security and Risk Analysis in Companies of Agriresort", *AGRIS on-line Papers in Economics and Informatics*, Vol. 9, No. 1, pp. 49 - 55. ISSN 1804-1930. DOI 10.7160/aol.2017.090104.

Introduction

Nowadays means of information and communication technologies represent a considerable advantage for anyone who can use them properly. Information society gradually changes business, public administration as well as each individual's life. This trend is evident also in a classic, and in many ways relatively conservative branch, such as agriculture (Šimek et al., 2008). Therefore it is also necessary to know how to protect and secure them properly. The term information security is often used in the relation to the information provided. Information security can be defined as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information (Whitman and Mattord, 2012). Following recent developments affecting the information security threat landscape, information security has become a complex managerial issue (Dor and Elovici, 2016). In business, but also in the overall economy we use information that can be regarded as an asset and it is therefore necessary to process and protect them. Assets ("asset") IS / ICT include the technologies, applications, data, and also people. Examples of the assets are hardware, software tools, data that the informatics uses and processes. It also includes the standardized and formalized processes and knowledge included in the informatics, as well as individuals such as operational staff, managers of individual applications, means of communication and other employees of the Department of Informatics (Gála et al., 2006).

The level of the usage of information and communication technologies (ICT) has a direct impact on the development and competitiveness of individuals, firms, production sectors, regions and even the whole continents. It is possible to state that the general characteristics and principles of ICT usage in the agriculture sector are beyond any doubt valid and will be valid in future (Jarolímek and Vaněk, 2003). Information assets are all processed data, equipment and people involved, or anything in the processing of information (Kaluža, 2006). Information assets are significant competitive and efficient sources of business in the globalizing knowledge economy. The significance of information security is therefore increasing. According to some other researches was also find that a risk taking firm may invest a larger amount in protecting and set than the risk neutral firm when the effectiveness of the investment in lowering breach probability is low (Mayadunne and Park, 2016). For evaluating the level of business information security there were created different methods to measure the effect of security. These

methods are dealt with by Kruger, Dervin and Steyn (2006). Their aim was to focus on areas of business that enhance information security - employees and their work with information.

Defining each level of information protection is quite difficult. Their vulnerability is on each level such as physical, organizational, procedural, personnel, management, administrative, also in terms of hardware and software (Oláhová, 2006). As stated in the document Information Security (2011), information security is achieved by implementing measures such as policies, processes, procedures, organizational structures and software and hardware functions. These measures must be implemented, monitored, reviewed and improved to fulfill the specific security and business objectives of the organization. It is also an information security from threats and vulnerabilities in order to ensure continuous and successful operation of the organization's activities to minimize business risk and maximize use of investment and business opportunities. Quality information and information technology must promote economic activity and this approach prevents their security (Kučera et al., 2009). Information security is not a management process that directly produces a profit, but they are necessary prerequisite for direct profit making processes. The aim of information security is to reduce the possibility of applying the threats and in case they appear it is to minimize their impact.

The properly defined security policy of the company is closely connected with the right implementation of information security. Selection and implementation of security products require properly defined information security infrastructure in the organization. Security infrastructure is a combination of measures, laws, government processes and experience with technologies and products that provide information security of organization. The aim of this security are the measures to prevent problems, detect problems, and alleviate damage, delay the effects of errors and attacks. Security infrastructure must also set certain standards for the assessment of the relevant factors in assessing the effectiveness of technologies, products and processes (Tarimo, 2006). Minimizing the impact of risks is a priority of security policy. Security policy is a basic plan that determines the information and assets and benefits of property which belong to organization as well as the manner of their protection. The employees have to have common rules when using the information sources, i.e what is allowed and what is not. It must also include the security policy components of the information system such as hardware, software, data and users. A properly constructed security policy is the basis for the development of projects aimed at safety. To minimize the risk of illegal use or misuse of information resources of the organization, the security policy is the first one as a safety measure (Danchev, 2004). Providing the IS risk analysis is needed to establish an effective security policy. Other necessities are to identify information assets that need to be protected, why they need to be protected and how the protection will be implemented (Tóthová, 2006). Overall, risk management is the total process used to identify, control, and minimize the impact of uncertain events (Peltier, 2005). Identified threats and risks need to be accepted or corrected. The analysis of risks includes the analysis of assets, analysis of threats and vulnerability analysis (Loveček, 2006). Another view of the risk analysis is obtaining objective basis so that security measures can be designed. Risk analysis is the process of identifying risks, evaluation of their size and the identification of areas that need to be provided by security measures (Hofreiter, 2006). Detection of possible operational threats which come from business interruptions and their financial impacts create the basic unit of the risk assessment (Kostrecová, 2008). There are many risk analysis methods available today, and the main task for an organization is to determine which one to use (Agrawal, 2017).

Overall, the management of data security is difficult. Quality management requires a combination of technical and business skills and knowledge of people, many of them are not intuitive. The basis of the information security is the risk management. Any extensive modern network can be ensured without a thorough understanding of the risk management process. It is important to understand the information security as a complex process consisting of the before mentioned parts. Additionally it is necessary to determine the correct security infrastructure, define the security policy and especially to analyze security risks. Information security and the overall security of information systems have been analyzed by researches of many authors such as Carlsson et al. (2009), Hennyeyová and Depeš (2010), Hennyeyová et al. (2013), Šilerová et al. (2016), Šilerová et al. (2015) or Bilozerov and Isomäki (2012), which focused mainly on the electronic exchange of business information between enterprises but also involvement and raising awareness of managers about information security and partly served as inspiration for our research.

Material and methods

From the year 2012 to 2016 the Department of Informatics carried out a research on issues of information security and security policy in agrirezort enterprises. This paper presents the parts of the research focusing on the assessment and evaluation of effective and safe use of ICT. The questionnaire survey was evaluated with statistical methods for the detection of relevance and relations of the data collected to confirm or refute the hypothesis of statistical indicators. A total number of hypotheses was 8, two of them were chosen for this article:

Hypothesis 1: Form of ICT administration is related to the security and protection of the ICT.

Hypothesis 2: Implementation of risk analysis threatening ICT affects the security solutions and ICT security.

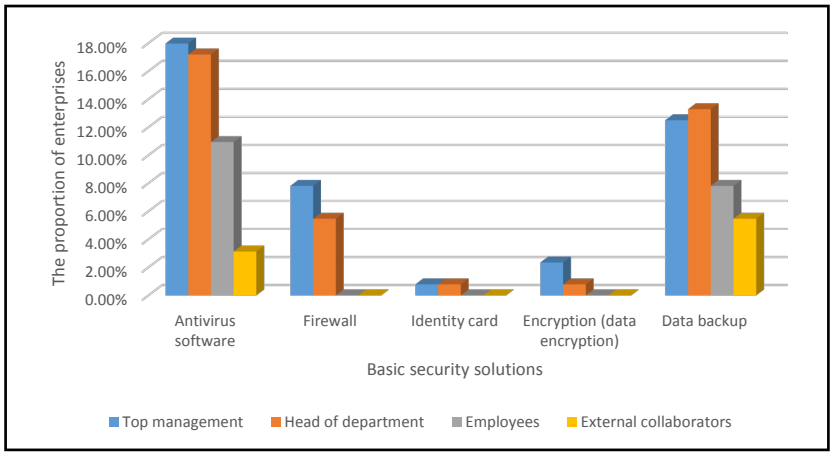
Several statistical methods have been used for the statistical evaluation. Verification of dependencies between the trait was carried out by use of chi-square test (χ^2), respectively. (χ^2) - square contingency. The test is based on comparing the theoretical and the empirical frequencies, e.i. which empirical frequency, if they were independent characters.

For the statistical analysis where the Chí-square test of independence could not be used, the Fisher's exact test was applied because the assumption numbers of cells in the pivot table was not followed. Fisher's exact test derives from the pivot table and verifies the null hypothesis of equality of the two units, namely the independence of two binary variables. This test is based on the assumption that all marginal frequencies (totals rows / columns) in the pivot table are fixed. This assumption is rarely met. They are mainly fixed in line frequency or in only the total frequency. If using the parametric methods was not possible because of failure in meeting the preconditions for their use, we applied nonparametric methods. Kruskal-Wallis H test is an extension of the Mann-Whitney test for three or more samples. The aim of the test was to find out whether the differences found in the sample medians of each group (according to the level factor) are statistically significant (between variables, the relationship) or could not be random (between variables, the relationship). The null hypotheses concerning equality of all medians was tested. If the P-value is lower than the chosen significance level (0.05), the null hypothesis is rejected. This means that the difference between at least one pair of median values calculated from the sample is too large, it can only be the result of random selection. Therefore it is statistically significant – there is the relationship between the variables. If the P-value equals to or is greater than the chosen significance level, the null hypothesis can not be rejected. This means that the difference between each pair of medians calculated from the sample can only be the result of random selection, therefore, not statistically significant – there is not the relationship between variables.

Results and discussion

The research sample consisted of 85% of cooperatives, 9% of joint stock companies and 6% of companies with limited liability. 69% of activities were in agriculture. The remaining businesses operate in the food industry. ICT security consists of items that the entity uses to ensure proper operation and protection of these technologies. All monitored entities have some form of security of ICT, especially at the technical level. This fact corresponds with the amount of funds spent on various forms of security and protection, the value of which is up to 500 EUR, while the survey shows that the vast majority of entities invest less than 1000 EUR for ICT in one year (40.63% enterprises). For other entities, it is smaller, but not insignificant amount because the adequate security and protection ICT cost less in opposition to the state of distortion of IS / ICT. According to the funds it is also important to know which organizational levels show interest in including the security solutions for IS / ICT. Research shows (Figure 1) that senior management has the greatest interest in the security solutions. It's relevant in incorporating ICT in the statutes, regulations, guidelines and regulations in the subject and their subsequent compliance.

ICT security does not fall only on the level of technical protection. An important part of the IS / ICT is non-technical protection presented as Security policy or project. The Security policy includes all the rules of the protection of IS / ICT as well as other assets of the company. Despite the fact that the Security policy and the Security project are the essential elements of asset protection in the enterprise, only a smaller proportion of companies actually create, apply and respect it. According to our research, 40% of subjects do not have these documents elaborated. Obeying the safety rules has important implications on how the enterprises manage their ICT. Usually in three ways, by internal employees, internal employees in cooperation

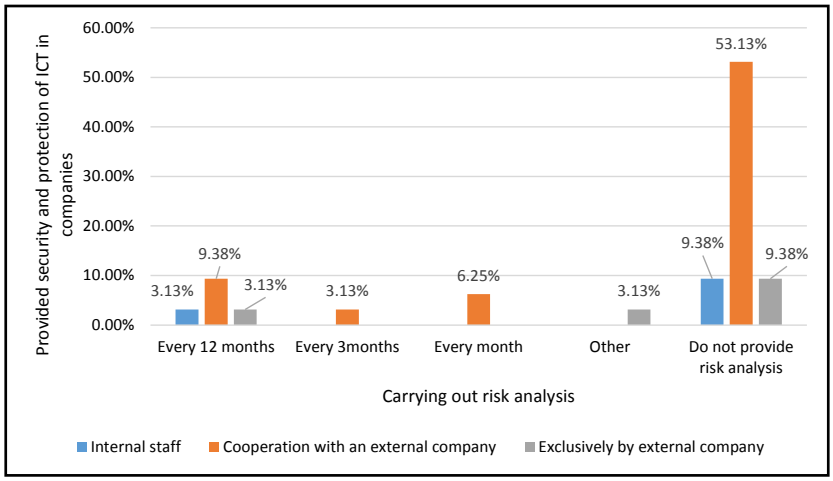


Source: own research and processing

Graph 1: Interest of the organizational levels in security solutions.

with the external company or solely an external company. The hypothesis 1 states how is the management of ICT related with enterprise security. The hypothesis 1 in this article was evaluated by using Fisher's exact test (for the Chí-square test of independence the assumption numbers of cells in the Pivot Table was not respected). The null hypothesis was formulated for the use of Fisher's exact test (H0: The form of management ICT and the protection and security of ICT is not statistically significant relationship.) and the alternative hypothesis (H1: The relationship between management of ICT and the protection and security of ICT is statistically significant.). Based on the Fisher's exact test P-value of the 5.167-13, and is thus lower than the significance level $\alpha = 0.05$. We accept the alternative hypothesis and reject the null hypothesis which means that the between the management of ICT and ICT security and protection is statistically significant relationship. Overall, the research shows that companies which have their own staff for ICT management are also responsible for ICT protection and security. On the other hand, companies that work with external companies for management of ICT cooperate with such companies also for ICT protection and security. Management of ICT by internal employees represents 6.25% of the companies; 3.13% in collaboration with an external company and 3.13% external company only. Although all parties ensure the protection of ICT, 71.88% of these entities does not perform an analysis of possible risks that may be threatening to their ICT. There also can be seen the connection between whether or not the businesses have own security policy or project. In this case the entities have the documents and they would follow the risk analysis in certain time intervals. Intervals of risk analysis directly derive from those documents and audit of information security. The hypothesis 2 in our article focuses on the analysis of risks and their impact on the security and protection of the ICT. The null hypothesis for Fisher's exact test was determined as follows: "There is not a statistically significant relationship between the implementation of risk analysis and management and security of ICT." The opposite hypothesis says that there is a statistically significant relationship. Based on the Fisher's exact test is the P-value 0.0095 and is thus lower than the significance level $\alpha = 0.05$. We reject the null hypothesis and accept the alternative hypothesis, so between the conducting a risk analysis of ICTs and solving the protection and security of ICT there is a statistically significant relationship. This is reflected on Figure 2, where the companies which cooperate with an external company in protection and security of the ICT do not perform risk analysis because they only focus on the situation, not on prevention. The relationship is visible, but it is negative more likely in agribusiness.

However it should be noted that companies should realize the importance of risk analysis. Without risk analysis the effective security measures in the organization can not be implemented. If such analysis is not part of building safety, it means that companies are not concerned with the security.



Source: own research and processing

Graph 2: The relationship between management of ICT protection and security and conducting a risk analysis of ICT in the company.

Conclusion

Many renowned authors state and confirm that the basis of adequate security environment of ICT should be directed by management of the company. This view can not be disagreed with. Peltier (2005) is indeed of the opinion that employees initiatively should encourage and highlight the potential safety risks of ICT in the company but confirms that the main proposals should come from top management. In all reported businesses the top management has the largest representation in protection and security of ICT. These forms of security are related to the funds that are spent and form part of the overall budget invested in ICT. The amount of about 500 EUR represents half of funds spent annually on ICT in the case of 40.63% of entities. For other entities, it is smaller, but not insignificant amount, as adequate security and protection of ICT represent lower costs in comparison to the situation of the violation of security of IS / ICT. Safety may not only be at the technical level, but may also be in the form of a document - Security policy or Security project, which form the base stone of ICT security in enterprises on non-technical level. However only a few entities have elaborated these documents Security policy (21.88%) and Security project (37.5%). ICT must not only manage but also provide the protection through either internal company employees (12.5%), in collaboration with an external company (71.88%) or exclusively external company (15.63%). Positive side, which can be noted after the survey, all parties address solve the protection and security of their ICT and leaves them in the risks and threats. Negative side may be finding that only 71.88% of entities does not perform an analysis of possible risks that may jeopardize their ICT. This can have a direct effect on the employees of the company and how they are informed about these risks. The vast majority of employees is not even aware of the security risks and the potential for ICT by businesses (11.72%). This is caused by the fact that these are the simpler systems and technologies that users commonly use in the private and therefore they expected to have basic knowledge of occupational safety and use of ICT. Finally, it is important to note that although they know the risks and try to develop security plans and projects, no ICT resources can be good in today's rapidly evolving technology for 100% protection.

Corresponding author:
Ing. Marcela Hallová, PhD.
Department of Informatics, Faculty of Economics and Management
Slovak University of Agriculture in Nitra, Tr. A. Hlinku 2, Nitra, 949 01, Slovak Republic
E-mail: marcela.hallova@uniag.sk

References

[1] Agrawal, V. (2017) „A Comparative Study on Information Security Risk Analysis Methods“, *Journal of Computers*, Vol. 12, No. 1, pp. 57-67. ISSN 1796-203X.

[2] Bilozerov, O. and Isomäki, H. (2012) „*Manager's information security awareness in Russian ICT small and medium sized enterprises*“, Jyväskylä: Jyväskylä University. 13 p. ISBN 978-8232-10090-3.

[3] Carlsson, B., Davidsson, P., Jacobsson, A., Johansson, J. S. and Persson, A. J. (2009) „*Security aspects on inter-organizational cooperation using wrapper agents*“, Ronneby: School of Information and Communication Technology. 14 p. ISBN 978-3642-01668-4.

[4] Danchev, D. (2004) „*Building and implementing a successful information security policy*“, Frame4 Security Systems Publications, Nov. 2004. [Online]. Available: http://www.windowsecurity.com/articles/Building_Implementing_Security_Policy.html [Accessed: 09 Dec. 2016].

[5] Dor, D. and Elovici, Y. (2016) „A model of the information security investment decision-making process“, *Computers & Security*, Vol. 63, November 2016, pp. 1-13. ISSN 0167-4048. DOI 10.1016/j.cose.2016.09.006.

[6] Gála, L., Pour, J. and Toman, P. (2006) „*Podniková informatika*“, Praha: Grada Publishing, 484 p. ISBN 80-247-1278-4.

[7] 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.

[8] Hennyeyová, K., Tóthová, D. and Hamášová, K. (2013) „Actual situation of risk analysis in enterprises of agrosector in Slovakia“, *8th International Conference on Applied Business Research* (ICABR). Brno, 2013, pp. 238-244. ISBN 978-0-620-55419-0.

[9] Hofreiter, L. (2006) „*Zásady a princípy analýzy rizík v oblasti fyzickej a objektovej bezpečnosti*“ Metodická príručka, May 2006. [Online]. Available http://www.nbusr.sk/ipublisher/files/nbusr.sk/oblasti-bezpecnosti/objektova-afyzicka/docs_of/analyza/zasady_metodika.pdf [Accessed: 08 Oct. 2016].

[10] Information security (2011) Virte, a.s. [Online]. Available: http://www.virte.sk/produkty-a-sluzby/informacna-bezpecnost [Accessed: 04 Aug. 2013].

[11] Jarolímek, J. and Vaněk, J. (2003) „The intensity and quality of Internet usage in the agriculture sector and possibilities of its further development“, *Plant, Soil and Environment*, Vol. 49, No. 11, pp. 525-529. ISSN 1214-1178.

[12] Kaluža, F. (2006) „Manažérsky prístup v riešení informačnej bezpečnosti firmy“, *Information Security, Security Revue – International Magazine for security engineering*. Vol. 6, [Online]. ISSN 1336-9717.

[13] Kostrecová, E. (2008) „*Informačná bezpečnosť 4, Klasifikácia a riadenie aktív*“. [Online]. Available: https://www.download.matus.in/Informacnabezpecnost/2008.04.ppt [Accessed: 11 Nov. 2016].

[14] Kruger, H. A., Drevin, L. and Steyn, T. (2006) „*A framework for evaluation ICT security awareness*“ North-West University. [Online]. Available: http://icsa.cs.up.ac.za/issa/2006/Proceedings/Full/17_Paper.pdf [Accessed. 25 Oct. 2016].

[15] Kučera, M., Repovský, A. and Fiľa, M. (2009) „Analýza bezpečnosti informačných systémov – súčasný stav v podmienkach agrorezortu na Slovensku“, *Acta oeconomica et informatica*, Vol. 12, No. 1, pp. 11-14. ISSN 1336-9261.

[16] Loveček, T. (2006) „*Bezpečnostná politika IT ako jeden zo základných dokumentov organizácie*“, Security revue. [Online], Available: http://www.securityrevue.com/article/2006/04/bezpecnostna-it-politika-ako-jeden-zo-zakladnych-dokumentov-organizacie [Accessed: 25 Oct. 2016].

[17] Mayadunne, S. and Park, S. (2016) „An economic model to evaluate information security investment of risk-taking small and medium enterprises“, *International Journal of Production Economics*, Vol. 182, pp. 519-530. ISSN 0925-5273. DOI 10.1016/j.ijpe.2016.09.018.

[18] Oláhová, E. (2006) „Počítačová bezpečnosť“, *Konkurencieschopnosť v EÚ - výzva pre krajiny V4 2006*: Medzinárodné Vedecké Dni. Nitra: Slovenská poľnohospodárska univerzita, pp. 1567-1570. ISBN 80-8069-704-3.

[19] Peltier, T. R. (2005) „*Information Security Risk Analysis*“, CRC Press, Taylor and Francis Group. ISBN 0-8493-3346-6.

[20] Šilerová, E., Pechrová, M. and Hennyeyová, K. (2016) „Utilization of cloud computing in Agricultural Holdings“, Scientific conference Agrarian Perspectives - *Global and European Challenges for Food Production, Agribusiness and the Rural Economy*, Sep 14-16, 2016, Czech University of Life Sciences Prague. ISSN 2464-4781.

[21] Šilerová, E., Hennyeyová, K., Vogeltanzova, T. and Junek, P. (2015) „ICT Influence on Supporting Agribusiness Development“, Scientific conference Agrarian Perspectives - *Global and European Challenges for Food Production, Agribusiness and the Rural Economy*, Sep 16-18, 2015, Czech University of Life Sciences Prague. ISBN 978-80-213-2581-4.

[22] 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 1214-1178.

[23] Tarimo, N. Ch. (2006) „*ICT security readiness checklist for developing countries: A social-technical approach*“, Stokholm: Stockholm University. 249 p. ISBN 91-7155-340-1.

[24] Tóthová, D. (2006) „*Počítačové siete v podnikaní v agrosektore*“, Vybrané otázky agrárneho práva Európskej únie III., [CD]. Nitra: SPU, pp. 105-106. ISBN 80-8069-812-0.

[25] Whitman, M. E. and Mattord, H. J. (2012) „*Principles of Information Security*“, United States of America: Boston, 601 p. ISBN-10: 1-111-13821-4.