RISK ANALYSIS OF A LOGISTICS COMPANY

LUCIE LENDELOVÁ

Abstract: *The purpose of this paper is to analyze risks associated with managing of information technology, including business, financial, technical, reputation and other risks. in one logistics company. The risks are identify and characterized in detail and are provided recommendations to remediate the situation and prevent the same type of problem (risk that problem can happen) that can occur in the company in the future. For the summarization of the risks and its impacts is created SWOT analysis. In this SWOT analysis are identify, describe and analyze strengths, weaknesses, opportunities and threats. Based on created analysis are give suggestions for other risks related to technology. Risk analysis is created from the view of an employee of this company, who is responsible for leading of project for development of new logistics information system.*

Keywords: *analysis, risks, information technology, logistics, recommendatons*

JEL Classification: *M21*

1. INTRODUCTION

This paper deals with a risk analysis of one logistics company. Risk analysis is focus on especially to risk related to technology, including business, financial, technical, reputation and other risks. The analyzed logistics company provides its customers complex logistics service which is on one hand based on warehousing in three temperature regimes (dry, cold, frozen) and also on to frozen of goods if it customers require and on other hand this company provides transportation of goods from customers to customers (for example from manufactures, to retailers, etc.). At first are identified and described some risks associated with technology and its importance in general context. After that are identified, described and analyzed risk associated with technology in logistics company and are provided recommendations to remediate the situation and prevent the same type of problem that can occur in the company in the future. The analysis is created by an employee of this company, who is response for leading of project for development of new logistics information system. This paper was created based on the instruction formulated in (Conduit, 2011; French, 2011).

2. IDENTIFICATION OF PROBLEM

In today's world give information technologies a considerable advantage for anyone. These technologies change gradually business, public administration as well as each individual's life. In some cases, is possible to observe of dependence on using of technologies (Hallové et al., 2017). Generally, companies use information technologies for optimizing processes, saving of costs and especially for gaining of competitive advantage. Within this context, outsourcing plays the important role and allows to extend the possibilities of sourcing through by using global sourcing of information and communication technologies resources (Prado, 2011). Regarding to its considerable and constant usage, there arise a question, how to protect and secure them. There exist some important terms: the term information security is often used in the relation to the information provided, the term Information security is possible to define as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information. The problem is that although managers know the risks and try to develop security plans and projects, no Information technologies resources can be good in today's rapidly evolving technology for 100% protection. Currently, information security is a complex managerial issue (Hallové et al., 2017). The importance of information technology is constantly growing and the failure of technology can cause a lot of problems and often cause significant impacts on shareholder value (Parent & Reich, 2009).

Parent & Reich (2009) identified five interrelated categories of risk (Fig. 1). They have developed a typology of IT Risk that can be governed at the Board level.

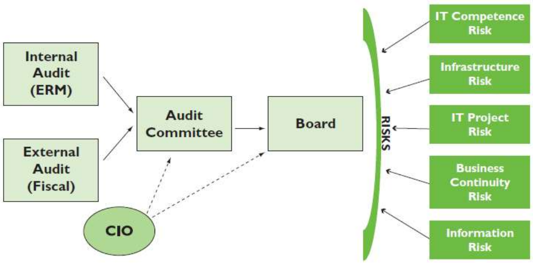

Figure 1 Typology of IT Risk
Source: Parent & Reich (2009)

The detailed view on the risks related to systems integration are very good illustrated in the hierarchical holographic modeling framework for identifying the source of software risks in systems integration (Fig. 2). Each of the seven visions solves multiple categories of risk sources. There exist many couplings and dependencies between categories and individual risk sources (Rich et al., 2000).

Finally, it is possible to note that, given the growing importance of information technology, it is also necessary to identify the risks associated with the use of information technology and to define a strategy for their elimination. This research problem is addressed by a lot of authors.

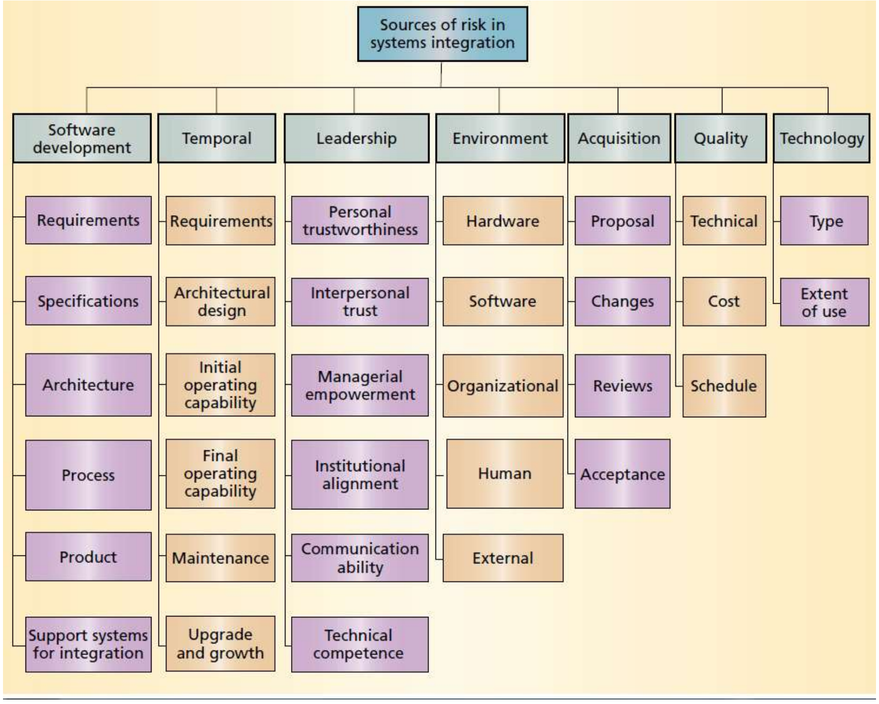

Figure 2 Hierarchical holographic modeling framework
Source: (Rich et al., 2000)

3. ANALYSIS OF CASE STUDY

This chapter analyzes the case of one logistics company, which is characterized in the introduction. There is created risk analysis with focus on risk related to information technology.

Based on risk analysis is possible to determination to what extent risks might affect company. It is possible not only identify risks to which a company is exposed but also to assess potential impact of those risks on the company. The aim of risk analysis is to identify and measure the risks associated with different activities in order to inform decision making (risk analysis, 2014).

Risks related to information technology that were identified in monitored company are listed in the table below (Tab. 1). There is also listed the probability of risk (P, scale is 1-5) and the severity of the risk (S). In provided risk analysis (Tab. 1) the author of this paper gave also a recommendation for improving.

Based on above listed risk analysis focus on information technology is possible to create SWOT analysis. In this SWOT analysis are identify, describe and analyze strengths, weaknesses, opportunities and threats. Created SWOT analysis (BusinessPundit, 2016) consists from these points:

Strengths

- Stable and functioning IT system and technology
- Existence of IT systems for warehousing, transportation, etc.
- Employees who work in company for long time know IT systems that are in company and are able to work with these systems in professional level
- In company exist manuals for using IT systems
- Etc.

Weaknesses

- Low level of maturity of system
- Low level of compatibility between IT systems
- Low level of IT governance
- Low level of data security
- Hardware is insufficient on some departments
- Changes in current IT systems is not possible
- Low flexibility of systems

Opportunities

- To increase the maturity of system
- To increase the IT governance
- To ensure high flexibility of systems
- To ensure compatibility between systems
- To develop new logistics system for planning in cooperation with university
- To include IT technology costs as a mandatory item in the budget and generate some money for IT technology
- To create company culture that will support managing with technology and train employee with IT technology
- Etc.

Threats

- Attack of terrorists
- Loss of data, disclosure of data, leakage of data
- System failure
- Obstacles of business operations
- Interruption of delivery of goods, delay of deliveries
- Loss of customer confidence, loss of customer
- Bad reputation
- Failure in developing of a new system
- Etc.

Table 1 Risks related to IT

Source of danger	Specifics and causes of danger	P	S	Risk level	Control measures, monitoring, verification of the functionality of the control measures and proposal for the adoption of recommendations
The company's spaces	**Specifics:** Security failures - possibility of intrusion of unauthorized persons **Causes:** Low security level The IT system is missing Employee negligence	2	1	2	**Current measures, monitoring:** Fencing and lighting of the area The entrance is fitted with a barrier Security service - continuous operation Camera system Keys issued against signature Entry into the warehouse based on chip card Identification of employees by personal cards Identification of visitors by cards Entry of visitors and external staff only with accompanying of employees **Recommendation: Implementation of an IT system for detecting people's intrusion and tracking their movement**
Machine room - cooling equipment	**Specifics:** There is no cooling of warehouses **Causes:** Intentional sabotage - shutting down the cooling equipment, setting the wrong temperature Engineer ignorance - setting of bad temperature Machine failure	3	5	5	**Current measures, monitoring:** Existence of an IT system for cooling monitoring and control, fault reporting, leading of records Engineer properly trained - machine operator, use of IT system, temperature requirements on individual chambers The presence of machine room staff from 6:00 to 18:00 h From 18:00 to 6:00 the machine room is locked Faults reported automatically by the IT system Signaling with red light at the concierge Determined crisis plan and procedure Regular maintenance and revision of the IT system **Recommendation: IT system reports faults only to the gatehouse, there is no existence of report that identify a shutting down of cooling system by engineer for long time. It is necessary to add to the system.**
Elektricity	**Specifics:** Power failure, blackout - non-functioning of IT systems, computers, machinery and refrigeration in warehouses and IT systems for operational management (transport and storage) **Causes:** External influence - blackout caused by the supplier Internal influence - blackout due to excessive power consumption, poor handling of electrical equipment	2	5	4	**Current measures, monitoring:** The regular inspection of electrical equipment. A working procedure for the handling of electrical equipment has been developed. Possibility to use a spare electric power source - generators Calling the crisis team and implementing the various remedy (ensuring that the temperature chain is not damaged, that the warehouses are closed, that the operation is operational) **Recommendation: to provide a more efficient generator for generating electricity.**
Technology equipment (hardware)	**Specifics:** Insufficient number and maturity of technical equipment **Causes:** Limited purchase due to limited funds, expensive technical equipment, uniqueness, badly defined system of recovery	3	3	3	**Current measures, monitoring:** Gradual renewal of technical equipment (computers, generators, cooling, etc.) Developed a rolling recovery plan **Recommendation: Track the technical state, renewal where it is needed**
IT systems	**Specifics:** Fault in the IT system **Causes:** Non-updated software, hardware, mechanical damage to the server	3	4	4	**Current measures, monitoring:** Regularly update software Errors and faults are reported instant
IT systems	**Specifics:** Low maturity of information systems, flexibility, inability to work with a large amount of data **Causes:** Obsolete IT systems No updates Lack of funding	3	3	3	**Current measures, monitoring:** Make regular updates Include financial IT requirements in the budget **Recommendation: To increase the level of maturity, purchase additional modules, or exchange systems for a complex integrated system that will be able to handle large or unlimited data**

Source of danger	Specifics and causes of danger	P	S	Risk level	Control measures, monitoring, verification of the functionality of the control measures and proposal for the adoption of recommendations
IT systems	**Specifics:** No compatibility between current IT systems **Causes:** There exist different IT systems from different supplier, implemented in different time.	4	3	4	**Current measures, monitoring:** Hiring more employees who try to eliminate discrepancy between IT systems. They create some reports and inform particular departments. **Recommendation: to implement one integrated complex system, for example SAP**
Data, Information Technology, access rights	**Specifics:** Misuse of business data, "crash" into the system and deliberate or unintentional interference with information systems, electronic data, access passwords **Causes:** Low level of data security Employee negligence Sabotage of employees	3	5	5	**Current measures, monitoring:** Set up of access rights Data are stored only on the server Data backup, anti-virus protection settings The existence of a description of a workflow for managing and backing up data in electronic form The room with the servers is locked, accessed by an employee of the IT department (key to the concierge against signing) **Recommendation: To increase of data security - Revise access rights, increase security of the server where data is stored, purchase better antivirus protection, improve room security with servers for example via ID card - eliminate human factor failure - release the key from the server room to unauthorized person.**
Human resources	**Specifics:** Lack of qualified employees, their ignorance of IT systems, difficult and long-term integration of new employees **Causes:** Lack of human resources Insufficient system of training	3	3	3	**Current measures, monitoring:** Existence of training system Existence of manual for IT systems **Recommendation: To create two different manuals, one will be very easy with pictures and second will long and there will a lot of detail of IT system.**

Source: Documents of monitored company

4. ALTERNATIVES AND RECOMMENDATIONS

Recommendations for current risk analysis were described directly in provided risk analysis. The author of this paper recommended also to identify and complete risk analysis by these risks:

- Limited financial resources for purchase of new hardware, IT system, actualization of current IT systems. In selected company is for example problem with planning of transport routes. it is necessary to include IT technology costs as a mandatory item in the budget.
- Development of new system – risk related to correct specification of system, requirement on system, others. When will company create own new logistics IT system is necessary to set up correct specification and requirement to the system, to ensure a compatibility with other systems that are currently use (for example warehousing system), to consult the development with experts and pay attention to other important issue associated with development of new logistics system.
- Outsourcing of IT system. There are also some risks related to outsourcing of IT system, for example problems with security, etc.
- Interruption of delivery of goods, limited business, delivery late caused by fault in IT system, blackout, hackers, etc.
- Loss of trust of customers
- Loss of reputation

Generally, the problems associated with IT technology are limited financial sources, time, people, business environment, safety, corporate culture.

5. CONCLUSION

In this paper was analyzed case of one logistics company in terms of risks associated with managing of technology, including business, financial, technical, reputation and other risks. Risks were identified, described and were give recommendations to eliminate of these risks. By using SWOT analysis were determinate strengths, weaknesses, opportunities and threats. Based on created analysis were give suggestions for other risks related to technology.

This contribution/publication is the result of the project **Centre of excellence for systems and services of intelligent transport II.,** ITMS 26220120050 supported by the Research & Development Operational Programme funded by the ERDF.

"Podporujeme výskumné aktivity na Slovensku/Projekt je spolufinancovaný zo zdrojov EÚ"

REFERENCES

[1] BusinessPundit: **SWOT analysis:** ***What is it and how to use it***? (2016). Chatham: Newstex.

[2] CONDUIT, S. (2011). ***PM Case Study Instructions.*** Emailed.

[3] FRENCH, J. A. (2011). ***Utilizing case study analysis in online learning***. CreateSpace. Chapter 21.

[4] HALLOVÉ, M., POLAKOVIC, P., VIRÉGH, R., & SLOVÉKOVÉ, I. (2017). ***Information security and risk analysis in companies of agriresort.*** AGRIS on-Line Papers in Economics and Informatics, 9(1), 49-55. doi:http://dx.doi.org.proxy.cityu.edu/10.7160/aol.2017.090104.

[5] PARENT, M., & REICH, B. H. (2009). ***Governing Information Technology Risk.*** California Management Review, 51(3), 134-152.

[6] PRADO, E. P. V. (2011). ***RISK ANALYSIS IN INFORMATION TECHNOLOGY AND COMMUNICATION OUTSOURCING/ANÁLISE DE RISCO NA TERCEIRIZAÇÃO DA TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÃO.*** Journal of Information Systems and Technology Management: JISTEM, 8(3), 605-618. Retrieved from http://proxy.cityu.edu/login?url=https://search-proquest-com.proxy.cityu.edu/docview/1011329519?accountid=1230.

[7] Rich Pethia, Clyde Chittister, Yacov Y. Haimes, Thomas A. (2000). Longstaff, ***"Are We Forgetting the Risks of Information Technology?",*** Computer, 33, 43-51, doi:10.1109/2.889092.

[8] ***risk analysis.*** (2014). In Qatar Financial Center, & Qatar Financial Center (Eds.), QFinance: the ultimate resource (5th ed.). London, UK: A&C Black. Retrieved from http://proxy.cityu.edu/login?url=http://search.credoreference.com/content/entry/qfinance/risk_analysis/0?institutionId=4966.

Lucie LENDELOVÁ, Ing., Ph.D., MBA
University of Žilina, Faculty of Informatics and Management Science, Department of Managerial Theories
Univerzitná 8215/1, 010 26 Žilina, Slovakia
e-mail: lucie.jelinkova@fri.uniza.sk