INCREASING COMPETENCIES OF SECURITY AND SAFETY MANAGERS IN THE RISK ASSESSMENT PROCESS

Andrej Raffaj¹, Katarína Kampová²

Abstract

Security management is an important part of the overall management of an organization. It aims to protect the health and life of persons, organization property and the environment itself. Achieving this goal, which represents achieving the required level of both security and safety, is undoubtedly dependent on the activities performed by security and safety managers. One of the basic processes affecting the security and safety level in the given organization is a risk assessment process. Based on the results of this process, particular measures are implemented to either avert or reduce the security and safety risks. The KARS method presented in this article is one of the methods applicable to the risk assessment process. The added value over other methods used in practice is that the assessment takes into account the correlation of the assessed risks. The case study presents the application of the KARS for evaluating risks magnitude within a real reference object.

UDC Classification: 376, **DOI:** <https://doi.org/10.12955/pss.v1.72>

Keywords: KARS method, security, assessment

Introduction

Security management is a complex process dependent on the competencies of a security and safety manager. Every one of them has to know various methods that can then be used for managing risks. The Kars method is a useful method within risk assessment. Therefore, we feel the urge to explain this method in our article as closely as possible which can be beneficial for broadening the theoretical knowledge of security and safety managers.

Security management meanings

Every organization that wants to be successful must be prepared to protect all the assets that represent and create values for the organization. Svetlik (2017) states that protecting workers, information, technology or property is an essential part of the organization because it needs to be effective and competitive. In order to ensure the stable and sustainable organization security and safety, it is important that a systematic management mechanism is put in place. This mechanism serves to ensure the proper functioning and development of the organization in accordance with all security requirements resulting from the relationship with state institutions, the competitive environment, suppliers, customers, employees, and also the responsible relationship of the given organization to environmental protection. Security and safety management, as one of the approaches to management, focuses on actions and activities related to protecting these values. It is not only focused on the product transformation process, creating products, nor on the service-providing process, or only on crisis management, but is focused on managing of the support activities. These activities are vital to the organization in terms of achieving the goals that have been set (Velas, 2016).

Security management addresses security issues in all sub-sectors of the security sector of an organization, especially security and safety of:

- persons - for example, health and safety at work, protection of personal data, physical protection of persons, etc.,
- property - object protection, protection of critical infrastructure objects, protection of information and information systems, protection against severe industrial accidents, protection of classified information, protection of business secrets, etc.
- environment - water protection, air protection, soil protection, etc.

This assurance is realized through a security and safety management system which has been designed and then implemented. This system corresponds to the capabilities, needs, environment and requirements of the maximum protection level of the organization that was explored by both Rehak (2019) and Hofreiter (2015). In practice, this system is usually made up of the purposeful arrangement and the use of available human resources, technical means, organizational and regime measures. The

¹ Ing. Andrej Raffaj, University of Žilina, Faculty of Security Engineering, andrej.raffaj@fbi.uniza.sk

² doc. Ing. Katarína Kampová, PhD., University of Žilina, Faculty of Security Engineering, katarina.kampova@fbi.uniza.sk

major premise for an effectively designed and implemented security management system in a given organization are the competencies of the security and safety managers.

Security management competencies

The level of security and safety in the given organization is influenced by various factors that affect it, whether from the external or internal environment. Nowadays, when the market is globally interconnected, there is much more factors that increase the amount of risks affecting organizations than in the past. This is one of the reasons why both Boros (2018) and Lovecek (2016) consider requirements for the competencies of security and safety managers as crucial and yet increasing.

As Mika (2006) states, for basic competencies the skills, knowledge and experience that the security and safety manager has acquired over the time and is able to use within his practice are considered. Weber (1990) introduces the three levels of security and safety manager competencies that are presented in Figure 1.

The social maturity of a security and safety manager represents the basic norms of behavior. According to Velas (2016) and Lovecek (2017) these norms are reflected in the manager's personal attitudes acquired through their education and upbringing and influenced by innate qualities as well. Expertise covers the appropriate knowledge that is necessary for the manager to effectively manage the organization's security and safety in perspective of organizational preparedness, time and cost effectiveness and technical efficiency of implemented measures. This knowledge is gained through adequate education and practical experience in this field. Practical skills represent the manager's ability to use expertise and perform his function effectively (Belan, 2015).

The security and safety manager competencies are directly applied in the process of risk assessment. The risk assessment is an essential precondition for the implementation of effective measures leading to enhancing the overall organization security and safety (Lovecek, 2016, Kampova, 2012, Boros, 2019). Therefore, the risk assessment is becoming an increasing challenge for security and safety managers. Due to changes in the environment, there are new forms of risks which are difficult to quantify due to the absence of necessary statistical data. The magnitude of such risks needs to be assessed differently. The solution to this problem is to raise the awareness of qualitative risk assessment methods. One of the qualitative risk assessment methods is called the Kars method.

Kars method and its theoretical explanation

Zakovsky (2015) defines the Kars method as a qualitative assessment tool for measuring the magnitude of risks. This method takes into account the correlation of risks. This correlation is determined with a pairwise comparison of each pair of risks which have been identified. By using this method, one is trying to determine when the exposure of a particular risk occurs. Also there is a presumption that a single risk or plenty of them will be induced.

In order to obtain a qualitative output Jelsovska (2013) proposes to keep the following steps:

- The identification of risks must be comprehensive and takes into account activities, aim and the internal and external organization environment,

- The development of a correlation matrix where risks are recorded in the matrix, with the risk in the first row of Ri is simultaneously represented in the first column of Ry;
- An evaluation by pairwise comparison whether there is a possibility that the risk Ri can induce other identified risks Ry (i,y = 1,2...n). If risk Ri has the potential to induce risk Ry, value 1 is entered in the matrix, otherwise value 0 is allocated. On the main diagonal of the matrix, value 0 is marked because, the risk cannot be induced itself,
- after pairing the row and column sums for each risk, these values are used for calculating activity and passivity coefficients.

The activity coefficient represents the percentage of the risks that may be induced by the risk Ri. Conversely, the passivity coefficient expresses the percentage of risks that may induce the risk Ry. The following relationships are defined to calculate activity coefficients:

$$KA = \frac{\sum 1Ri}{\text{All risks} - 1} \times 100 \quad [\%] \quad (1)$$

$$KP = \frac{\sum 1Ry}{\text{All risks} - 1} \times 100 \quad [\%] \quad (2)$$

This method also includes a graphical representation of the magnitude of the analyzed risks. First, the activity coefficient values are applied to the x-axis, and the individual risk factors passivity values to the y-axis. The locations of the O1 and O2 axes are then determined. Their position will allow categorizing risks into 4 areas, namely:

- First area (I): risks with the primary and secondary magnitude,
- Second area (II): risks with the secondary magnitude,
- Third area (III): with the primary magnitude,
- Fourth area (IV): risk with the lowest magnitude.

For calculating the location of the axes, the following formulas are used:

$$O_1 = K_{AMAX} - \frac{K_{AMAX} - K_{AMIN}}{100} \times 40 \quad (3)$$

$$O_2 = K_{PMAX} - \frac{K_{PMAX} - K_{PMIN}}{100} \times 40 \quad (4)$$

The advantage of the method is that individual risks are not assessed in isolation, but the mentioned correlation is taken into account, which can be used to determine which risks should be dealt with priority in order to reduce them to the required level.

Risk assessment through the Kars method

The administrative building of Krpeľany Water Construction located in the Martin District of Slovakia was chosen as the reference object. Subsequently, a correlation matrix was created and all risks were paired to determine whether they have a potential to also trigger other identified risks or not. After this comparison, both row and column sums were obtained, which are then used for calculating the activity and passivity coefficients of each risk. The results of the comparison are shown in Table 1.

After being put into their respective relationships, for every individual risk, values of activity and passivity coefficients were obtained which express the correlation as a percentage. The coefficient values are presented in Table 2.

Table 1: Risk correlation matrix

RISK	R1.	R2.	R3.	R4.	R5.	R6.	R7.	R8.	Σ
R1 - Burglary - related theft	0	0	0	0	0	0	0	0	0
R2 - Fire due to welding	0	0	1	1	1	0	0	0	3
R3 - Fire of flammable substances	0	0	0	1	0	0	0	0	1
R4 - Fire of electric-wiring	0	0	1	0	0	0	0	0	1
R5 - Burning during welding	0	1	0	0	0	0	0	0	1
R6 - Eye damage during sawing	0	0	0	0	0	0	0	0	0
R7 - Head injury	0	0	0	0	0	0	0	0	0
R8 - Flood	0	0	0	0	0	0	0	0	0
Σ	0	1	2	2	1	0	0	0	6

Source: Authors

Table 2: Coefficients percentage values

Coefficient [%]	Risk							
	R1	R2	R3	R4	R5	R6	R7	R8
KA	0	42,9	14,3	14,3	14,3	0	0	0
KP	0	14,3	28,6	28,6	14,3	0	0	0

Source: Authors

The risk with the highest activity coefficient was classified risk 2 (R2). This risk has the potential to trigger 42.9% of all identified risks. Its exposure can only cause 14.3% of the other risks, which is declared by its passivity coefficient.

As soon as the location of the axes is calculated, the risks are classified into four magnitude areas which are illustrated in Figure 2.

Figure 2: Correlation graph

Source: Authors

In the context of qualitative risk assessment through the Kars method, the primary risk with the highest magnitude was evaluated as risk 2 (R2), which is capable of inducing the greatest domino effect of all identified risks when its exposure happens. Both risks R3 and R4 were classified as risks with a secondary magnitude. Risks that require the least attention are risks R1, R5, R6, R7 and R8. The Kars method creates the preconditions for a successful risk assessment process and allows security and safety managers the means for successful risk management.

Conclusion

Security management is an important part of the overall organization management. One of the basic conditions for successful risk management are security and safety managers who have the required competencies, not only in terms of expertise, but also in terms of a personal predisposition, namely their constant education. In the organizational environment new factors influencing changes in the environment that need to be integrated into risk assessment processes occur. In many cases, these factors are causally dependent and it is necessary to investigate and evaluate them, and by the appropriate methods consider these ratios. Realistic risk assessment is therefore becoming an increasing challenge for security and safety managers. In this article the Kars method was introduced, which has its place in security practice. This method integrates a causality of the studied environment and creates a simple tool for security and safety managers to get an initial overview of the interaction of individual risks. It also creates a prerequisite for assessing the potential domino effect of identified risks.

Supported by the VEGA project: 1/0628/18 Minimizing the likelihood of experts' subjective estimates in a security practice using quantitative and qualitative methods.

References

- Belan, L. (2012). Security management. Security and risk management. University of Zilina. ISBN 978-80-554-1138-5
 Boros, M., et al. Development of security at the local level through practical students training. 12th International Technology, Education and Development Conference (INTED), Valencia, SPAIN, 2018

- Boros, M., et al. Required competencies of security managers for decision-making. 13th International Technology, Education and Development Conference (INTED), Valencia, SPAIN, 2019
- Hofreiter, L.(2015) Security management of property . University of Zilina. ISBN 978-80-554-1164-4
- Jelsovska, K., Peterkova, A. (2013). Crisis resolution - methods and their applications. Retrieved from <http://projects.math.slu.cz/AM/activ/soubory/opory/reskrizi.pdf>
- Kampova, K., Lovecek, T. (2012). Managing security in organization. University of Zilina. 2012. ISBN 978-80-554-0615-2
- Lovecek, T., et al. Currently Required Competencies of Crisis and Security Managers and New Tool for Their Acquiremetn. 3rd International Conference on Management Innovation and Business Innovation, Manila, PHILIPPINES, 2016
- Lovecek, T., Ristvej, J., Magdolen, M., et al. Determination of Personal Data Sensitivity and Security Measures Assignment Conference: 4th International Conference on Management Science and Management Innovation (MSMI 2017), Location: Suzhou, Book Series: AEBMR-Advances in Economics Business and Management Research, Volume: 31, Pages: 1--5 , Published: 2017
- Lovecek, T., Ristvej, J., Sventekova, E., et al. Currently Required Competencies of Crisis and Security Managers and New Tool for Their Acquirement. Conference: 3rd International Conference on Management Innovation and Business Innovation (ICMIBI 2016), Location: Manila, PT 2 Book Series: Lecture Notes in Management Science, Volume: 58, Pages: 3--8, Published: 2016
- Mika, V.T. (2006). Management basics. Retrieved from <http://projects.math.slu.cz/AM/activ/soubory/opory/reskrizi.pdf>
- Rehak, D., et al. *Complex approach to assessing resilience of critical infrastructure elements*. International Journal of critical infrastructure protection, 25, 125--138, 2019
- Svetlik, J., et al. The safety training in the municipality. 9th International Conference on Education and New Learning Technologies, Barcelona, SPAIN, 2017
- Velas, A., et al. Education and lifelong learning opportunities in the private security services in Slovak republic. 8th International Conference on Education and New Learning Technologies, Barcelona, Spain, 2016
- Velas, A., Svetlik, J. Design of Equipment to Improve Safety on Roads. 20th International Scientific Conference on Transport Means, Juodkrante, Lithuania, 2016
- Weber, J. *Managerial value orientations: A typology and assessment*. International Journal of Value-Based Management, 3, 37--54, 1990
- Zakovsky, J. (2015). Use of geographic information systems in threat and risk mapping processes. Retrieved from https://digilib.k.utb.cz/bitstream/handle/10563/33882/%C5%BE%C3%a1kovsk%C3%BD_2015_dp.pdf?Sequence=1&isallowwed=y