Risk Assessment of Physical Security within a Technologized Knowledge Based Organization

Mihail Aurel Țițu^{1,*}, Alina Bianca Pop², and Costel Ceocea³

¹Lucian Blaga University of Sibiu, Victoriei Street no. 10, code 550024, Sibiu, România

²SC TechnoCAD SA, Vasile Alecsandri no. 72, code 430351, Baia Mare, România

³Vasile Alecsandri University of Bacău, 157, Calea Mărășești, Bacău, România

Abstract. The purpose of this scientific paper is to support the decision-making process on the risk management based on the results of an analysis and subsequently on the risks hierarchy. This assessment involves the comparison of the level of risk determined by the analysis with the risk criteria developed in the context of the establishment phase. This scientific paper on assessing and treating risks to physical security has been developed to identify, assess and quantify the associated risk in a technologized knowledge-based organization. The basis of this study on the assessment and treatment of risks to physical security is to identify specific potential risks as well as the emergency response procedures. Effective risk assessment involves assessing the likelihood and impact of a risk-based event, and based on the determined values, determine the risk profile and treatment priorities. The determined risk level is assimilated to risk exposure.

1 Introduction

The theory says a manager may have one of the following three attitudes to risk: risk taking, risk rejection, or risk indifference. When managing risk and wanting to respond to the three attitudes, business people's reactions may be as follows in figure 1.

Fig. 1. The business people's reactions.

*Corresponding author: mihail.titu@ulbsibiu.ro

The company in which the research related to this scientific work was conducted is part of the knowledge-based organizations. The main activity of this technologized organization is in the field of computer aided design. The mission of the organization is to design engineering products and services in the field of mechanical engineering (CAD), geographic information systems (GIS) and multimedia, training in assisted design and use of CAD engineering, promotion and marketing of CAD software quality, professional and competitively priced, so as to achieve a high level of customer satisfaction. Within the company, the establishment of security requirements, measures and mechanisms is closely linked to the risk assessment grid, the grid developed for this analyzed objective. The first condition to ensure a security climate is represented by the need for a qualified person (employee or consultant) to develop physical security procedures, to ensure their implementation and control. All materials and equipment used to ensure objective safety must be certified according to DE or national standards in force. Monitoring and intervention in case of events (burglaries, false alarms, etc.) will be done by the specialized company.

Fig. 2. The electronic security system.

Fig. 3. The tasks of the software programming of the electronic security system.

The configuration of the mechanical and explosion protection systems is established based on the risk analysis and the minimum-security requirements set out in the methodological norms of GD 301/2012 [1]. Mechano-physical protection involves a number of elements that ensure physical delimitation of unauthorized access to existing values. Their role is to protect the life

and integrity of the operating personnel [2-4]. The degree of safety/strength of the mechano-physical protection equipment used in organization is determined in proportion to the amount of protected values and the level of risk determined, and it is recommended to choose an average level class defined by European/national standards. The electronic security system must be designed to perform the following functions presented in figure 2.

The software programming of the electronic security system envisages the tasks [5, 6] presented in figure 3.

2 Policies and responsibilities regarding the physical security of the organization

Within the analyzed organization, a set of physical security measures and procedures are implemented and appropriated by staff. There is a person designated by the company to be responsible for security to process security procedures and verify compliance.

The attitude of the organization concerned to the identified risks associated with its activity, the establishment of the security mechanism and the risk criteria are in accordance with the legal provisions set out in the Minimum Security Requirements for Category of Organizations in Annex no. 1 to GD no. 301/2012 [1], as well as according to the working methodology present in the MAI Instructions no. 9 / 01.03.2013 [7].

The identified risk sources within this company are presented in figure 4 as follows:

Fig. 4. The identified risk sources.

The leaders of organizations possessing goods and values have the obligation to identify and establish functional areas corresponding to their activities and to take the necessary measures to ensure the protection of life, the integrity of persons and the security of values. (Annex No. 1, art. 1 of GD No. 301/2012) [1]. Areas of impact in the event of a security incident specified in Annex I, GD 301/2012 [1] and identified in the organization under review are:

- Unit access area and perimeter area (Aap) - The area of access to the unit means the place provided with non-structural closures designed for entry or exit of persons. Access paths can be dedicated to customers, employees, transfer of values or mixed. The perimeter area is the physical limit of the building, consisting of fixed or movable elements, such as walls, glazing or windows.
- Storage area (As) - is the space specially designed to safely store monetary values or goods stored in the lens.
- Security equipment area (Ase) - is the restricted area of unauthorized access for the location, operation, or monitoring of such equipment.
- Other High Security Areas (Ahs) - Areas requiring restrictions or special protection due to protected values or activity.

In a security incident, depending on the nature and intensity of the incident, the following consequences are taken into account for this organization:

- Human nature: Incidents that may result in loss of life or endanger the integrity and freedom of individuals and may have a major impact on society.
- Material: Theft or theft of goods, values or information within the unit, destruction of goods, damage to electronic components of security systems, installations or other existing equipment, vandalism of equipment, destruction of perimeter areas of buildings, disruption of lines communication, fires, floods.

3 Working Methodology

In order to assess the physical security level of an organization, two areas of physical security risk, i.e. the acceptable security risk associated with security risks with estimated values below the critical threshold of 60%, and the unacceptable risk associated with the values above the critical threshold, are established. It is considered that the legal requirements of physical security for an organization are met if the assessed risk falls within the acceptable security risk.

The security level grid includes four categories of analysis criteria:

- a) objective specific criteria, which assess the area and local location elements with a weight of 25%;
- b) security criteria, which assess the security measures implemented or to be implemented, with a weight of 65%;
- c) functional criteria, which evaluate the elements regarding the performance of the activity of the evaluated organization, with a weight of 10%;
- d) other non-grid criteria that provide assessment of other elements that impact on security risks, grouped into growth and risk mitigation categories.

Completing the rating grid is done by selecting an option in the "Variables" column for each item, and entering the data in the table of information for other criteria as expected.

By completing the rating scale, the value in the column "Total score" on the "Weighted Score" column, which is the value associated with the determined degree of risk, is obtained. The total score is calculated by the application by summing the weighted values under the headings: Goal, Security Criteria, Functional Criteria, and Other Criteria on the "Weighted Score" column. Higher score values indicate a high level of risk of physical security events occurring. The weighted value for each item evaluated is provided by the application by applying a percentage coefficient of the maximum value associated with the item in the "Associated Score" column, the weight resulting from choosing a variation from the "Variables" column, depending on the analyzed situation. When completing the assessment grids, account is taken of the requirement to meet the minimum, general and specific security requirements, recorded in the grid in the "assessment elements" column, for which the corresponding minimum score option is associated in order to continue and complete the assessment. In order to determine the level of threats, the specific crime coefficients are calculated, calculated at county and area level, based on the statistical data registered by the criminal and operative records structures of the IGPR, the Public Order Directorate and the police inspectorate of the county to which the organization belongs, on crimes perceived by robbery and thefts of companies, registered in the previous year. Specific crime rates are classified in the following areas:

- a) high crime rate for counties / areas with coefficients above the national / county average;
- b) average crime rate for counties / areas with coefficients with values between 75% - 100% of the national / county average;
- c) Low crime rate for counties / areas with coefficients below 75% of the national / county average.

The accessibility element is evaluated by site inspection in the immediate vicinity of the objective, in order to identify all access paths that make it possible to leave the area quickly. It is believed that there is a possibility of rapid collapse / escape from the area of the lens if within a

radius of 10 m from the entrance there are access ways that make it possible to leave the area in at least three different directions of movement (gangs, passages, walkways, etc.). The possibility of average concealment / escape shall be considered for the purposes for which, within a radius of 25 m from the entrance, access routes are identified which allow the area to leave in at least three different directions of movement. In other cases, the possibility of concealment / escape is considered to be cumbersome. From the point of view of neighborhoods, the evaluation is done by identifying the units close to the target and verifying the existence, type and functioning of the security devices at them. Neighborhood score is determined by choosing the relevant identified option in question by analyzing the existing units within a range of 25 m from the evaluated one. An evaluated organization that has no other objectives within a 50 m radius is considered to be isolated from the neighbor's point of view. For this organization, the assessment and quantification of grid factors is done through local appreciation of the state of fact and by consulting security service contracts, transport values, monitoring, installation and maintenance of alarm systems, procurement documents, certification, functional and functional checks of electronic equipment and mechano-physical protection equipment.

4 Risk Analysis

The identified risks associated with the organization's activity, as well as their impact areas, were recorded in Table 1 of the Risk Register.

Table 1. Risk Register.

No	Risk Code	Name of the risk	Impact areas			
			Aap	Ad	Ase	Asr
1	R1	Attack / Armed robbery	x	x	x	x
2	R2	Intrusion	x			
3	R3	Robbery		x	x	x
4	R4	Assaults on individuals		x	x	x
5	R5	Acts of disturbing public order	x			x
6	R6	Destruction / Vandalism	x	x	x	x
7	R7	Ignorance / failure of security procedures	x	x	x	x

The identified risk analysis was performed using the risk-matrix matrix. The level of risk was expressed within the combination of plausibility of the risk and its consequences. Thus, the related scores are:

- Probability (P): 5 - almost certain; 4 - Probably? 3 - possible; 2 - unlikely; 1 - rare;
- Impact (I): 5 - catastrophic; 4- major; 3 - moderate; 2 - minor; 1 - insignificant;
- Risk (R) (probability x impact): 15-25 very high; 8-12 high; 4-6 medium; 1-3 low;
- Plausibility scale according to incident, probability and quantification: rarely - 0.1-19.99% every 30 years; unlikely - 20-39.99% every 3 years; possible - 40-59.99% once every 100 days; probably - 60-79.99% once every 10 days; Certain 80-99.99% once a day.

Impact scale:

- Insignificant - without personal injury, loss <1000 EUR, without interruption of services;
- Minor: no personal injury, loss 1000 - 10000 EUR, short-term activity, up to 2 hours;
- Moderate: injuries requiring first aid without hospitalization, losses> 10000 EUR, discontinuation of work up to one day, investigations by the authorities;
- Most: injury to one or more people with hospitalization, loss of more than 10000 EUR, total disruption of activity for 1-5 days, investigations by the authorities;
- Catastrophic: death of one or more persons, loss of more than EUR 100000, presentation of the media event at the national level, investigations by the authorities, interruption of activity for more than 5 working days.

Table 2. Analysis of identified risk types and functional areas in terms of history and estimates.

Risk	Aap			As			Ase			Ahs		
	P	I	R	P	I	R	P	I	R	P	I	R
R1	2	2	medium	2	3	medium	2	3	medium	2	3	medium
R2	2	2	medium									
R3				2	3	medium	2	2	medium	2	3	medium
R4				2	3	medium	2	3	medium	2	3	medium
R5	2	1	low							2	1	medium
R6	2	2	medium	2	2	medium	2	3	medium	2	3	medium
R7	2	3	medium	2	2	medium	2	2	medium	2	2	medium

5 Conclusions

The risk assessment involves comparing the level of risk determined during the analysis process with the risk criteria established in accordance with Law 333/2003 [8], Minimum Requirements for Unit Categories specified in GD 301/2012 [1], and according to the Grid No 7 of the level of risk to fit into the acceptable risk area. The risk assessment of physical security makes use of the risk underlying the risk assessment in order to make decisions about future actions. Legal, financial, and other ethical considerations, including perceptions of risk to physical security, are also considered to contribute to decision-making. The treatment of the above risks will be done through the implementation of new mecano-physical security measures, security systems measures, measures with human staff, or policies, responsibilities and functional measures.

Within the organization, there are implemented security procedures employed by employees that include instructions on the use of security systems as well as instructions on how to act in the event of a security incident. According to the data publicly available on the Romanian Police site, the target is 2017 as having a specific crime rate at county level of 62.70 having a domain of framing the level of low crime, and at the level of locality of 1393.86% having an area of high crime criminality. The objective was assessed according to the risk level grid for areas larger than 500 m² according to the MAI no. 9 of 01.03.2013, resulting in an acceptable level of risk of 52.00%.

References

1. H.G. nr. 301/2012 *pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor si protectia persoanelor*, 11.04.2012

2. F. Cantelli, N. Kodate, K. Krieger, *Questioning world risk society: three challenges for research on the governance of uncertainty*. Glob Policy (2010)

3. J.R. Aiello, C. M. Svec, J. App. Social Psychol., **23**, 7, pp. 537–548 (1993)

4. B. J. Alge, J. Appl. Psychol., **86**, 4, pp. 797–804 (2001)

5. M.W. Allen et al., Management Communication Quarterly, **21**, 2, pp. 172–200 (2007)

6. M. Donner, IEEE Security and Privacy, **1**, 3, pp. 6-7 (2003)

7. Instrucțiuni nr. 9 din 1 martie 2013 *privind efectuarea analizelor de risc la securitatea fizică a unităților ce fac obiectul Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor*, 01.03.2013.

8. Legea nr. 333/2003 *privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor*, 08.06.2003.