

DOI 10.20544/HORIZONS.A.27.4.20.P03
UDC 351.746.3:005.51]:323.285}:005.52:005.334

SAFETY RISK ASSESSMENT OF TERRORIST ATTACKS WITHIN PLANNING IN PRIVATE SECURITY¹

Assoc. prof. dr. Ice Ilijevski

Faculty of Law, University "St. Kliment Ohridski" - Bitola

iiljevski@hotmail.com

Dr. Kire Babanoski

kbabanoski@gmail.com

Prof. dr. Zlate Dimovski

Faculty of Security - Skopje, "St. Kliment Ohridski" - Bitola

zdimovski@fb.uklo.edu.mk

Abstract

The private security personnel make a significant contribution to counter-terrorism initiatives. Covering up a large number of operational positions in the facilities, the security personnel can provide early warning and recognition of risks and threats from possible terrorist acts.

In order to identify the risks, threats, vulnerabilities, and dangers of terrorist attacks, it is necessary to make a safety risk assessment before the security process begins, more precisely when the security operational plan is being compiled.

The safety assessment of risks and threats is an extremely important component to enable private security staff to successfully manage the security challenges that arise and to ensure a consistently best level of protection for individuals and facilities. Safety assessment of risk and threat levels allows private security staff to plan reactive actions in a timely manner and be properly prepared if certain security events occur.

Keywords: risks, threats, dangers, security assessment, terrorist attacks

¹ original scientific paper

INTRODUCTION

The terrorism is a global threat to all mankind, which leaves especially negative and harmful consequences. The terrorist organizations have their own ideology and they tend to achieve their goals in every possible way. For this purpose, they recruit, train and include suitable members in their organization, whose main characteristics are the different types of fundamentalism and radicalism. The activities of the terrorists - the members of the terrorist organization, are committing terrorist acts in order to cause fear and insecurity among the population and in the public, to overthrow the state order, and thus extortion of certain behavior by the government, in order to achieve their political, religious or ideological goals.

With the accelerated development of the private security in the country in the last years, the number of public and private buildings and properties whose security is taken care of by private security agencies is increasing. Within the scope of the working tasks and competencies, the private security personnel apply the given competencies in order to secure the property and the people from any internal or external threats and dangers. The so far forms of endangering the security of the property, the objects and the people were attacks, thefts, sabotage, destruction, damage, etc., but recently new hybrid threats have emerged that could significantly endanger the customer safety. The terrorist attacks, incidents and actions are form of security threat whose ways of conducting are different and are constantly changing. They are real and quite serious in terms of the consequences they can create. The attacks can occur at any place, in any time without warning to the organization and the people in it. The terrorism is not just a violent act toward the people and the property. Damage or destruction of the communication systems, damage of the assets and the working equipment and destroyed reputation can cause rapid and/or long-term damage to the businesses and are therefore equally desired and applied by terrorist organizations.

The fight against the terrorism is highly dependent on the effectiveness of the measures and the activities taken by the law enforcement agencies, their speed in detecting the terrorist organizations, their preparatory actions and their

actions after a terrorist attack. The fight against the terrorism requires close co-operation between such entities for the purpose of exchanging information and timely detection of illegal activities that precede the terrorist acts.

The private security system plays a very important role in both preventing and dealing with critical incidents, including terrorist attacks. They are the first to be able to provide assistance after the incident. Therefore, the private security personnel need to upgrade their knowledge, skills and abilities to protect the property, the buildings and the people from all kinds of modern forms of endangerment. They must be able to recognize, warn and point out the suspicious activities they observe during their work, as well as to take appropriate measures and activities to prevent emergencies and protect them from occurring.² This means that their work tasks should be targeted before and after the incident.

SAFETY OPERATIONAL PLAN

In terms of security protection activities, safety plans or security plans³ are prepared. Each type of security has its own characteristics that need special attention, in addition to the common features in the application of the appropriate measures defined by the security operational plan⁴. It is a key document in the process of preparing and implementing all security-related activities. Such a document is compiled for all places that are used regularly and are continuously analyzed and supplemented. All agreed measures determined by the plan are implemented conscientiously, responsibly and in a disciplined manner, regardless of whether it is an individual or joint activity (which includes a certain coordination and synchronization).

² Илијевски, И., Димовски, З., Бабаноски, К., Обезбедување на лица и објекти, Комора на Република Македонија за приватно обезбедување, Скопје, 2018, p 25

³ Белић, М., Васић, М., Историјско-правни аспект послова обезбеђење одређених личности и објеката, Безбедност, часопис Министарства унутрашњих послова Републике Србије, Београд, 1-2/2009, стр. 114 и Павловић, Н., Модели праћења и процењивање безбедносне ситуације у функцији обезбеђења и заштите одређене личности, специјалистички рад, Криминалистичко-полицијска академија, Београд, 2013, p. 19

⁴ Jakić, M., Preventivna delatnost u zaštiti lica, 18.01.2012, from <http://vipprotection-miloradjakic.blogspot.com/2012/01/>

Security plan means assessment of the security situation for the endangerment of the secured object, ie the person and the security measures that are being prepared and undertaken.⁵

Before starting the process of securing the person and the object, a realistic assessment of data on occurrences and events related to their safety must be made. By monitoring the bearers of the threats, their influence, force and means of use, should be created and taken measures for elimination or removal of the circumstances in which they were created.

Based on the observations and the knowledge from the security situation, first, the already existing types of endangering life, health and actions of persons are determined, and then, depending on the work it deals with, the political views and other characteristic data, are assessed the security threats and the consequences that could arise in the future.

The security assessment is determined in the form of a written document and is an integral part of the security plan. It shows the current security situation, forecasts events and specifies the tasks to eliminate the causes, methods of suppression, ie prevention of endangering safety of the person and the object. The security protection plan is a comprehensive and concise document that enables and supports the distribution of information to all hired private security personnel.

The information in the security plan are the basis for the operational plan, which should reduce or eliminate the danger or counter the identified risks and provide guidance to the private security personnel in the case of an incident.

Types of plans:

- Permanent plan;
- Temporary plan.

Each plan is different based on the specific requirements of a particular place. For that reason, the plan should be and remain flexible, because in almost all cases something extra can happen and, in that case, certain measures and activities will have to be changed. The goals of strategic planning are to preserve the safety of the protected person and the building. For better prevention, concrete plans are being made.

When preparing a security plan, it is important to keep in mind that there are key and backup plans. The plan should always be maximalist, ie the security

⁵ Станковски, Љ., Планови за обезбедување и процена на безбедносната ситуација, Меѓународно научно списание за одбрана, безбедност и мир, Современа македонска одбрана, Министерство за одбрана, Скопје, 2013, p. 138

should be planned with, as far as possible, stronger measures. Basically, it starts with the maximum security plan and then adjusts depending on: the material capabilities, the existing needs, the freedom of the client's private life, the conduct of his regular activities, but never adjusts to the extent that it would drastically endangered the safety of the person and the object. The plan must be realistically feasible and as simple as possible.

The security plan should be informative, integrated and multi-layered.⁶

The business companies cannot eliminate all the threats they face, so they need to have a plan to protect their most valuable assets and they have to plan ahead and prepare their response to major incidents and breaches of their security and reliable operation.

The security planning must not be developed in an arbitrary or ad-hoc way, nor must it be developed solely from the previous mistakes and omissions. To be effective, the security plan must be built based on the information about almost every aspect of the work in the present, but also in the future. It must be fully integrated with the daily operations, the supply chains and the routines. It should be "multi-layered" - where each measure is reinforced by the next one.

The structure and the concept of the plan differ from one organization to another, but each plan should generally consist of the following components:

- Information: assessment of the business activity and the environment in which it operates - threats, risks, hazards, vulnerabilities, most valued and most critical assets.
- Protective safety: measures against identified threats and vulnerabilities.
- Planning response: the way the organization will react in the event of a breach.
- Security culture: building security awareness throughout the organization.

The large, multi-sector organizations can create separate plans for each location in order to reflect the local structures and activities, in addition to a comprehensive plan that outlines the common activities and interdependencies.

The security plan should be a working document where every aspect is constantly revised and updated in response to the organizational change. In the larger organizations, such a role can be assigned to a staff member who is part of the organization's management or who is directly responsible to the

⁶ Centre for the Protection of National Infrastructure, Protecting against terrorism, third edition, 2010, p. 5-6

management, with the support of a specialized team. In the smaller organizations, this should be someone with a similar status and understanding of the business. Regardless of the size of the organization, the plan must have the full support of the senior management and to be communicated throughout the business, especially when certain staff members have delegated responsibilities. In the event of an incident, the competence of those responsible for coordinating the response must be clearly understood by all employees.

Sharing tips and information is an important part of any security plan. The opinions of the senior management and employees of the organization are essential. But just as important are the contributions of those outside the business, such as emergency services, neighboring businesses and specialist experts (structural engineering, information technology, etc.).

The security plan contains some of the most sensitive information available to the business and it is therefore important to be clear about who has full access and how it is distributed.

THREAT IDENTIFICATION

Some business activities are "at greater risk"⁷ than others because of the services they provide, their relatively high percentage, or the number of people assigned to them. The organizations need to know the range of threats they face - both direct, where business is the target, and indirect, from relatively weak, to catastrophic threats.

The organizations need to constantly check what is relevant to their work or which circumstances may put the staff or the key assets directly under threats. For example:

- What is the nature of the business or services it offers?
- Is there something on the spot that can be an important goal, e.g. materials, machinery, resources, data, plans, technical expertise?
- Is the business related to a highly professional person or to a disputed area of work?
- Does the organization maintain visibly high security standards?

In short, how likely is it that the organization/company, or staff, could be a direct target of a pre-planned attack?

⁷ Centre for the Protection of National Infrastructure, Protecting against terrorism, third edition, 2010, p. 7-8

There may also be indirect influences that are results from an attack elsewhere - where the organization itself was not the target but suffered the consequences.

For example, are the business premises located near a high-risk building? If so, how would it affect the operation if it could not be accessed for a few days? Will the staff be able to travel if the local transport network is severely disrupted? Can information and technology networks react to the sudden appearance of a new virus or vulnerability? Can an incident in another city or country cause significant problems for suppliers, customers, or the delivery of basic materials? The other social factors can also increase the threats to the organizations. Do the workplace safety concerns increase the employees' risk of stealing or selling/leaking information?

SAFETY RISK ASSESMENT

The safety assessment means a set of knowledge and conclusions that are acquired from the participation of certain entities and are evaluated in an appropriate procedure.⁸

The assessment of the security situation is a link between the collections, analysis and processing of the data on one hand and making decisions on the other hand, in order to be prevented the security breaches of the people.⁹

The security decisions need to consider threats, vulnerabilities and potential impacts. It is always not practical to pay much attention to fully protecting every aspect of the organization. Instead, the important decisions about safeguards or changes in the procedure should only be made after a full risk assessment. This includes a strategic analysis of threats, vulnerabilities and potential consequences¹⁰ for the organization in order to be identified the most important risks on which the resources should be focused. The risk assessment

⁸ Стајић, Љ., Пајковић, Д., Систем заштите личности и објеката, Правни факултет, Нови Сад, 2008, р. 86

⁹ Крстић, С., Безбедносна процена угрожености одређених личности, Миленијум груп, Београд, 2012, р. 65

¹⁰ Centre for the Protection of National Infrastructure, Protecting against terrorism, third edition, 2010, р. 11-12

should not be limited only to information obtained exclusively from internal resources. The external sources of information should also be used equally.¹¹

The risk assessment process involves logical assumptions about the likelihood of a threat and its potential impact if the current security measures fail to protect it. The areas at risk can be defined by several criteria: population, accessibility, criticality (towards everyday life), economic impact, and symbolic value. The identification of such vulnerable areas should be coordinated with the state security services.

There are different ways to conduct a risk assessment and each organization should use its own methodology as appropriate, but the process should probably be based on the following principles:

1. Identify your key assets.

The first step for the organization is to use the information gathered in assessing the threats to identify the potential risks, ranging from catastrophic to relatively minor:

- Bomb in or near the entrance of the main building..
- Suspicious package received by mail.
- An employee who uses his or her access to issue and sell specific confidential information.
- Virus entered in the main information system.
- An employee discreetly transfers small funds to an unauthorized account.

2. Compile a simple indicator to indicate the potential impact of each incident.

This indicator should be based on the assumption of the consequences, ie how a certain event will affect the business activity (eg whether it can cause injuries and casualties, impact on productivity, damage to the reputation and trust of the client, etc.).

An appropriate scale for the organization should be used, e.g. from a "5" result for the worst possible outcome - it is almost certain that lives will be lost or buildings will be destroyed - to a "1" result if it is likely that the incident could be easily controlled or repaired at low cost and without publicity.

3. For each scenario, a second indicator is placed, which is a probability that the incident will occur at a certain location.

¹¹ Димовски, З., Бабаноски, К., Илијевски И., Заштита при терористички напади, Комора на Република Северна Македонија за приватно обезбедување, Скопје, 2019, p. 34

It should be considered why and how it can happen and how the existing security measures should be realized.

A similar consistent scoring system should be applied to the above, such as "1" ("extremely unlikely") to "5" ("safe"). For example, the probability of petty theft may reach "5", but the chances of detecting an explosive device in the building may reach "1".

When the two ratings for each scenario are compared to the other scenarios, the threats that the organization needs to focus on begin to be revealed. It can help if the 5x5 matrix points are drawn using impact and probability as axes. The best practice is to look at the results yourself, for each scenario separately - without multiplying each other, as this can obscure the results (eg petty theft can carry the same 5x1 points as a 1x5 bomb).

LEVEL		CONSEQUENCES				
		5	4	3	2	1
P R O B A B I L I T Y	5	Red	Red	Red	Yellow	Yellow
	4	Red	Red	Yellow	Yellow	Yellow
	3	Red	Yellow	Yellow	Yellow	Green
	2	Yellow	Yellow	Yellow	Green	Green
	1	Yellow	Yellow	Green	Green	Green

Table no. 1. Matrix for determining the level of security risk

These results are only indicative, and any pre-planned activities may still cover more than the probability or impact, but this process should help focus on finding concrete solutions. This exercise should be reviewed regularly so that all changes in the threat and vulnerability can be taken into account.

CONCLUSION

No matter what approach is used, categorizing the threats is of great importance for security risk assessment. The risks could be grouped in the following categories:

- Protection: areas where changes or improvements are necessary in current measures, either through new equipment or through procedures.
- Adaptation: risks that can be reduced through operational changes, e.g. outsourcing, change of routines, etc.
- Acceptance: risks are rated as minimal when mitigation/change costs outweigh the costs.
- Unpredictability: risks that will require plans to provide an alternative or reserve - especially assets that are considered essential to operations.

From this point of view, the organization should consider safeguards that can protect its interests and response plans to ensure that the security personnel deal effectively in the event of any incidents.

BIBLIOGRAPHY

1. Белић, М., Васић, М., Историјско-правни аспект послова обезбеђење одређених личности и објеката, Безбедност, часопис Министарства унутрашњих послова Републике Србије, Београд, 1-2/2009
2. Centre for the Protection of National Infrastructure, Protecting against terrorism, third edition, 2010
3. Димовски, З., Бабаноски, К., Илијевски И., Заштита при терористички напади, Комора на Република Северна Македонија за приватно обезбедување, Скопје, 2019
4. Илијевски, И., Димовски, З., Бабаноски, К., Обезбедување на лица и објекти, Комора на Република Македонија за приватно обезбедување, Скопје, 2018
5. Крстић, С., Безбедносна процена угрозености одређених личности, Миленијум груп, Београд, 2012
6. Стајић, Љ., Пајковић, Д., Систем заштите личности и објеката, Правни факултет, Нови Сад, 2008
7. Станковски, Љ., Метод на изработка на безбедносна процена како функција на безбедносниот менаџмент на претпријатијата, Меѓународен годишник на Факултетот за безбедност – Скопје, 2012

8. Станковски, Љ., Планови за обезбедување и процена на безбедносната ситуација, Меѓународно научно списание за одбрана, безбедност и мир, Современа македонска одбрана, Министерство за одбрана, Скопје, 2013