CHANGE OF SOFT TARGET'S RESILIENCE IN TIME – CASE STUDY

DORA LAPKOVA & LUKAS KRALIK

Abstract: *This article is focused on Soft targets, especially on change of Soft target's resilience in time. We present our case study. We try to find the possibility how to calculate and to find out the resilience in time. When we want to protect Soft targets, this knowledge is very important for us. We use the process, which we presented in another article [1] and here, we demonstrate the practical using. For our research, we chose the school, and with help of Event tree analysis (ETA) we are showing the whole process.*

Key words: *Soft targets, case study, risk analysis, Event tree analysis, attack*

Authors´ data: Lapkova, D[ora]; **Kralik**, L[ukas], Tomas Bata University in Zlín, Zlín, Czech Republic, dlapkova@utb.cz; kralik@utb.cz

This Publication has to be referred as: Lapkova, D[ora] & Kralik, L[ukas] (2019). Change of Soft Target's Resilience in Time – Case Study, Chapter 15 in DAAAM International Scientific Book 2019, pp.199-204, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-24-2, ISSN 1726-9687, Vienna, Austria DOI: 10.2507/daaam.scibook.2019.15

1. Introduction

The Soft targets [2] are very important security theme, which solves many security experts. The terrorist attacks are in many places, and the effectivity of attack is too high. We try to find new possibility how increase our protection and how set up the security measures. Many objects have risk management in their process, so we use this system in another way. Ob. Cit.: "As "Soft Targets" can be referred to those objects, (open) spaces, or events characterized by the accumulation of a large number of people, the absence or low level of security measures against violent assaults and their omission among critical infrastructure and hard target objects." [3]

In the first part, we explain the methodologies – risk analysis and their division. In the second part, we describe the case study using one of the risk analysis - ETA.

2. Methodologies

The initial step for finding resilience is a risk analysis and security audit. In this case study, security audit is omitted and the emphasis is placed on analysis to describe step-by-step what should happen when soft target is endangered.

2.1 Risk analysis

Risk analysis can be perceived as a technology to understand how different dangers act to the subject. No risk analysis can practically detect system dangers, since the analytical output is always partly true and partly hypothetical, as it is based on many factors. Risk analysis is always based on teamwork and is part of emergency and crisis plans. Therefore, the first step is the risk reduction process and the second step is risk management.

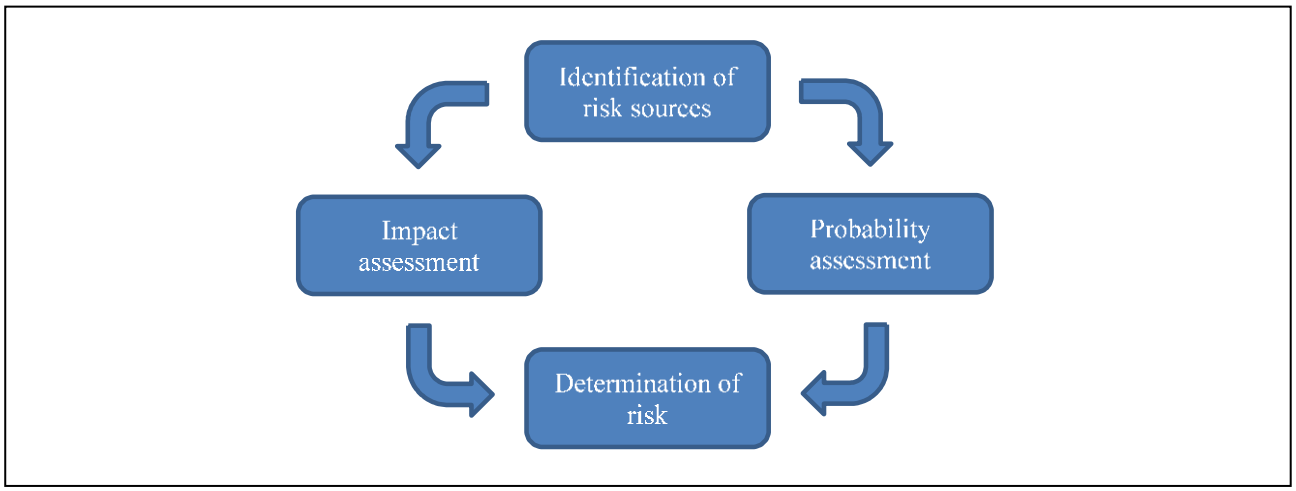

Fig. 1. Risk source model [4]

Risk analysis typically includes the following activities:

1) Identification of risk sources – this part includes the following activities:
   a) Establishment of baseline data – data about the analysed subject, description of operation, location, etc.

b) Identification of assets - definition and determining the value of assets that the subject own;

2) Identification of threats – identification of events and actions that may affect negatively the value of assets;
3) Identifying of vulnerabilities – every asset has own vulnerability or weakness against the identified threat. The level of this vulnerability affects the impact when threat affect the protected asset;
4) Determining and assessment of impact.
5) Determining of risk – determining the probability of occurrence threats and vulnerability rates of the subject. [4]

2.2 Division of risk analysis

Risk analysis can be carried out by various methods. It always depends on the decision evaluator and needs for which the analysis is intended. According to the general classification, there are two basic approaches to the solution - quantitative method and a qualitative method. However, it is not excluded the possibility of using a combination of both approaches. Individual methods are described below.

Quantitative methods

With this method, risks are calculated mathematically and based on the frequency of the threat and its impact. The method uses a numeric valuation if the event is likely to occur, but also in appreciating the impact of this event. The risk is most often expressed in the expected form losses in financial form. These methods are more qualitative than those exact. The implementation of these methods requires more time and effort, but they provide financial resources the expression of risks, which is more favourable for better risk management. The disadvantage of this method It is not only an effort and time but also a highly formalized procedure that can lead to failure to capture the specificities of the subject under assessment. This can lead to high vulnerabilities. This is due to the "overload" of the evaluator with a large volume of formally structured give [5]. Some quantitative methods:

- Preliminary Hazard Analysis (PHA)
- Process Quantitative Risk Analysis (QRA)
- Failure Mode and Effect Analysis. (FMEA)

Qualitative methods

In this method, the evaluator shall also take into account the duration of the hazard and the size of the space, in which the danger can be realized. As time or space increases, it grows as well as risk probability. The number of hazards that an object or object must also be mapped the process is exposed because the hazards may be interdependent (perfectly or partially), which means that if one hazard is the source of another hazard, then it is one danger. The number of hazards can serve as a guide for processors analysis, which cannot be the output of analysis.

As already mentioned, risk analysis need not be divided only in quantitative and qualitative terms. It is possible to combine both approaches to achieve a better result. [6]

Some quantitative methods:

- Event Tree Analysis (ETA)
- Safety / Security Review (SR)
- What – If Analysis (WIA)

Event tree analysis

Event tree analysis is a procedure that tracks the progress of a process from the initiation event. The branching events is always based on two options - positive and negative. The ETA method is a graphical-statistical method. System view the event tree is a branched chart with agreed symbolism and description. It shows all events that may occur in the system under assessment. As the number of events increases, the resulting graph gradually branches as tree branches.

Safety/Security Review

Comparative method using inspection routes where the systematic assessment of selected aspects of the system (eg operational activities) is carried out by means of control procedures, records, standards, etc. It usually complements other techniques for identifying risk sources. The result is a qualitative description of possible safety problems and incentives to remedy them.

3. Case study (attack in school by knife)

This part of the paper discusses and analyses the security breach scenario with respect to the soft target resilience. The analyzed event is based on real events, which are typical for schools around the world. It is an attack on student and school employees by a knife. This incident should be described in 6 phases:

1) Intrusion into object
2) Attacker merge with a group of students
3) Support for integration into a group of students
4) Conflict
5) Attack
6) Reaction

Threat: deliberately attacking a group, under threat of a knife attack on a selected student

Characteristics: The attack is carried out by a foreign visitor to the object for whom the object is not intended. The attacker in his appearance and age corresponds to a characteristic group of students. Uses uncontrolled entry into the object. At the beginning of the semester, he will get involved in teaching a selected group of students several times. After a certain period, he identifies how to perform the attack. The reason for the attack is the need for recognition and the influence of drugs.

Asset: Teachers, students, and other staff.

Description of harm: The harm may affect the mental and physical health of the persons in the building. There is a risk to the health and life of a person or a group of persons at the same time.

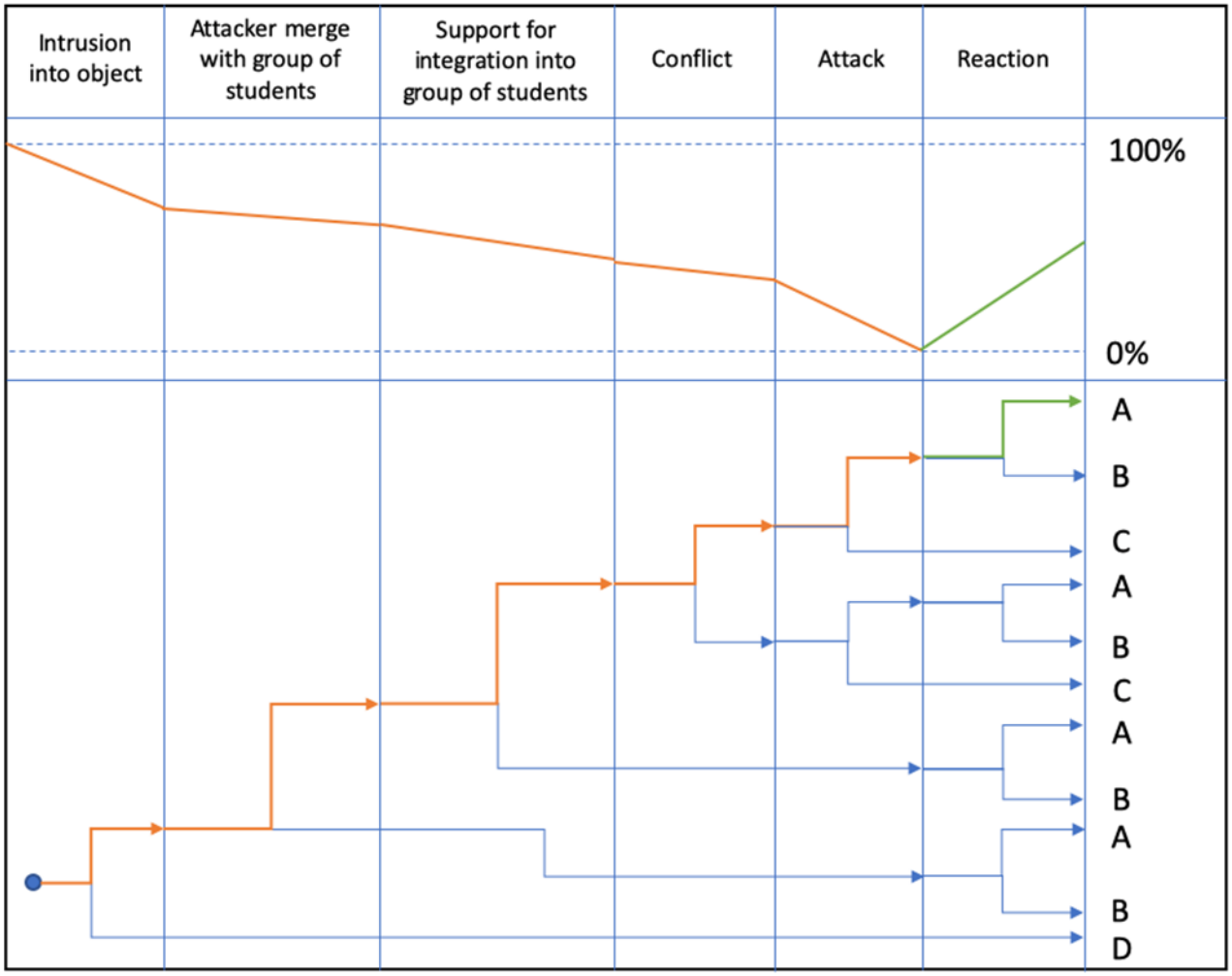

Fig. 2. ETA with resilience change in time

The result of ETA is shown on fig. 2. Incident described in this case study is highlighted because there are 4 possible conclusions:

A. The attack was performed, however, impact as injuries and loss of life were minimalized thanks to proper reaction.
B. The attack was performed, catastrophic impact on human lives; not proper or no reaction.
C. The attack was not performed; the attacker was stopped in time.
D. Best conclusion when the attacker is not able to intrude into the protected object.

Every phase has a negative effect on overall resilience of Soft target. From initial event, the resilience is getting lower until the moment of beginning of an attack. At this moment is resilience equal to zero because all security measures fail and human lives are in direct danger. Proper actions may increase the level of resilience. How to calculate and determine the current level of resilience is described in different part of the research [1].

4. Conclusion

This article was focused on the change of Soft target's resilience in time. With the help of the ETA we described the practical using of the process of finding out the actual resilience. In security, there are very important to know the actual situation in protected object (building, event etc.) because then we can react. The protection of Soft targets is very complicated, there are many factors which influence it. The more information helps us to react correctly and in time of need.

5. Acknowledgements

This work was supported by the research project VI20172019073 "Identification and methods of protection of Czech soft targets against violent acts with elaboration of a warning system", supported by the Ministry of the Interior of the Czech Republic in the years 2017-2019 and also by the Ministry of Education, Youth and Sports of the Czech Republic within the National Sustainability Programme project No. LO1303 (MSMT-7778/2014) and also by the European Regional Development Fund under the project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089.

6. References

Lapkova, D., Malanik, D., Kralik, L. and Kotek, L. (2019) Cybersecurity in Protection of Soft Targets. In: 2019 9th IFIP International Conference on New Technologies, Mobility & Security: Proceedings of NTMS 2019 Conference and Workshop. Canary Islands - Spain: IEEE eXpress Conference Publishing, s. 1-6. ISBN 978-1-7281-1541-2.

Lapkova, D., Kotek, L. and Kralik, L. (2018). Soft Targets – Possibilities of their Identification. In: Annals of DAAAM for 2018. VIENNA: DAAAM INTERNATIONAL VIENNA, s. 0-9. ISBN 978-3-902734-21-1. ISSN 2304-1382.

Kalvach, Z. (2017). Definition of Soft Targets. Prague.

Svobodova, A. (2012) Risk analysis of dilapidated buildings in Svit Zlín (Analýza rizik chátrajících budov v areálu Svit Zlín). Zlín. Tomas Bata University in Zlín.

Methods of risk analysis (Metody analýzy rizik). Promis [online]. [cit. 2019-10-11]. Dostupné z: http://promis.econ.muni.cz/lecture/2/5/1/

Cermak, M. Risk analysis: quantitative vs. qualitative (Analýza rizik: kvantitativní vs. kvalitativní). Clever and Smart [online]. [cit. 2019-10-11]. Dostupné z: https://www.cleverandsmart.cz/analyza-rizik-kvantitativni-vs-kvalitativni/

Lapkova, D., Malanik, Z. and Adamek, M. (2011). Use of the high-speed camera in self-defence. In Annals of DAAAM for 2011 & Proceedings of the 22nd International DAAAM Symposium "Intelligent Manufacturing & Automation: Power of Knowledge and Creativity". Vienna : DAAAM International Vienna, 2011, s. 1531-1532. ISSN 1726-9679. ISBN 978-3-901509-83-4.