BASICS OF SOFT TARGETS PROTECTION

GUIDELINES

Basics of soft targets protection - guidelines (2nd version)

Created by Ing. Zdeněk Kalvach et al., Soft Targets Protection Institute, z.ú.

Prague

June 2016

PREFACE TO the ENGLISH VERSION

This Guideline, written in 2015 – 2016, is the first resource material offering a comprehensive approach to the protection of soft targets in the Czech Republic. The Guideline is applicable to all institutions and sites which are threatened by terrorist assaults but also to various types other soft targets, which may not represent a likely target for terrorists but which may face other violent attacks with comparable impact.

The protection of soft targets is a domain governed by the Ministry of Interior, namely the Security Policy and Crime Prevention Department of the mnistry. This Guideline has been created in close cooperation between this department and Zdeněk Kalvach, Director of the Soft Targets Protection Institute, and is based on long term security experience with various forms of protection of sites, communities and individuals against extreme assaults. Joint assessment of various security methods and examples of good practice provided a solid foundation for the final concept to be adopted by the Ministry of Interior at the national level. Therefore, the Guideline is a fine example of a successful PPP cooperation.

The whole concept is open to discussion and further amendments. We believe that it can serve as a useful resource not only in the Czech Republic but also in other countries. Despite differences in details, the underlying principles are globally applicable.

CONTENTS

INTRODUCTION

This document provides a guideline for the protection of the so called **soft targets** (see below). We focus on protecting the **individuals** from s**erious assaults** against **individuals** rather than the protection of private and corporate property,

The Guideline is applicable to attacks conducted by terrorists as well as aggressive extremists or individuals with criminal motives or even people acting out for purely personal incentives (e. g. an ex-employee) or mentally ill people. The Guideline can be adjusted to the needs of any institution (official or unofficial, such as a business, school, NGO, public organization or even a family) and any building (commercial, public, private).

The Guideline primarily deals with **prevention of potential attacks and mitigation of possible impact** because soft targets usually lack capacity to strike back against attackers and it is for the professionals provided by the government, community or, rarely, a private subject to take care of that.

Soft targets protection in the context of the national system of public order and safety protection and crisis management

The security measures adopted by soft targets are measures adopted primarily on voluntary basis by administrators / owners of soft targets. The purpose of these is not to substitute but to complement the national system of public order and safety protection stipulated by the State and articulated in laws.

The soft targets' need to create their own plans and procedures in case of a serious security incident results predominantly from the following two facts:

1. Certain incidents are not serious or significant enough to entitle the potential target to demand state sponsored security measures. And yet, some soft targets consider such incidents a serious threat to regular operation and want to address them correspondingly. For example when a school has to handle a serious school-bus accident or when a business needs to react to escalated security situation in the neighborhood.

2. Security (emergency) plans of soft targets play an important role in prevention (mainly due to raised security awareness and the training of the staff) and in the phase immediately after an incident, before the arrival of the Integrated Rescue System teams. Experience with terrorist attacks and active shooters shows that the first minutes and preparedness for immediate response play a crucial role in mitigating impact.

So far, private businesses had to rely on themselves which has given rise to a trend of setting up the so-called Business Continuity Plans (BCP), which assess the possible threats, including serious security incidents, and outline applicable procedures and solutions.

VULNERABILITY OF SOFT TARGETS

Recently, the security situation in Europe has been deteriorating. Terrorism and extremism have been gaining grounds and have shown a new trend of assaults which resemble terrorism because they hit soft targets and kill randomly but lack ideological motive. Strictly speaking, the Czech Republic has been so far spared terrorist attacks as such[1] but there is the infamous incident of arson driven by racism (i.e. extremist), motivation and targeted at a house inhabited by a Roma family in Vítkov (2009). We have also experienced attacks of „non-ideological" nature, such as the shooting in a restaurant in Uherský Brod (2015) or the attack with a knife and taking of hostages in a school in Žďár nad Sázavou (2014). Several other attacks, similar to those described above, were prevented or stopped in the initial phase.

All these attacks were beyond the standard self-help capacity of the attacked subjects and all exceeded the limits of common crime. Most of these incidents resulted in casualties, with consequences affecting the whole community. More often than not, coordinated effort was necessary to put recovery measures in place. The lesson we are learning is that terrorists are still more and more likely to attack unprotected places where people congregate, regardless of whether there is or is not a political, religious or other symbolic pretext (**i.e. the soft targets**).

The challenge for the State is that there are innumerable soft target areas. State agencies and public administration will never have the capacity to provide sufficient security for all possible locations. For this reason, the security measures adopted by soft targets themselves are becoming an increasingly significant component of public security. Many soft targets are even capable of ensuring better security for themselves (for example if they have greater resources – knowledge of the place, contacts, staff on the spot and financial funds etc.) than the State ever could.

Types of soft targets

There is no official definition for the term „soft targets". In the security circles, however, the term is used to denote **places with high concentration of people and low degree of security against assault**, which creates an attractive target, especially for terrorists. On the contrary, the so called "hard targets" are well secured and

[1] In modern history of the Czech Republic, only one person has been sentenced for a terrorist attack in accordance to § 311 of Penal Code. The convict had threatened the then Minister of Finance in a letter.

guarded premises (e. g. some government buildings, military premises, law enforcement offices as well as some well-protected and guarded non-governmental or commercial facilities).

Placing the soft targets in focus alongside the hard targets reflects an innovative attitude towards security management. We pay greater attention to the attackers' point of view and study the likelihood of an attack rather than its impact and social consequences. The main advantage of this approach lies in the fact that we provide security to subjects which would traditionally not have been entitled to protection – commercial facilities, community events, private individuals etc.

Typical soft targets include:

- schools, dormitories, canteens, libraries,
- religious sites and places of worship,
- shopping centers, market places and commercial facilities,
- cinemas, theatres, concert halls, entertainment venues,
- gatherings, parades, demonstrations,
- bars, clubs, dance clubs, restaurants and hotels,
- parks and squares, tourist monuments and places of interest, museums, galleries,
- sporting arenas and stadiums,
- important transportation sites, railway and bus stations, airport terminals,
- hospitals, medical centers and other health care facilities,
- public meetings, pilgrimages, fairs
- cultural, sports, religious and other events
- community centers

Selected types of soft targets in more detail:

Schools

Schools mean children. Children are associated with extreme vulnerability while at the same time they represent one of the most precious assets of each society. That is why attacks against schools are perceived as the most tragic ones. In the past, schools have been targeted by terrorists but also by students themselves, which calls for a multifaceted security approach.

Shopping centers

Shopping centers attract huge amounts of visitors and the security is usually very weak, which makes them a very good soft target. In the past there have been many tragic incidents in shopping centers. We have seen dramatic terrorist attacks in shopping centers using explosives, hostages etc. For example in the period between 1998 and 2005 there were more than 60 terrorist attacks of this type[2].

[2] RAND Corporation Study: Reducing Terrorism Risk at Shopping Centers, 2006. The total amount includes all documented attacks worldwide from 1998 through 2005.

Hotels

Hotels typically provide space for large amounts of people. The threat of an attack becomes more likely when a hotel houses for example a security-risk conference or other function. Attackers may also be drawn to the owner(s) of the hotel or by the national profile of hotel guests.

Sports and cultural events

Security measures have become an indispensable part of big social or sports events open to the public. However, organizers rarely provide more than a very basic event management, with most attention paid to demarcation of restricted zones and abiding to organizational rules. We need to acknowledge that events of a certain nature require a more profound security backing. Especially, if there are many participants and if the event is covered by the media or held in high-risk places at high-risk times.

Religious (today in CR it is mainly Jewish) premises and places of worship

Religious (in CR typically Jewish) premises and places of worship represent a specific category of soft targets attracting the attention of Islamic terrorists and extreme-right activists.

Transportation sites

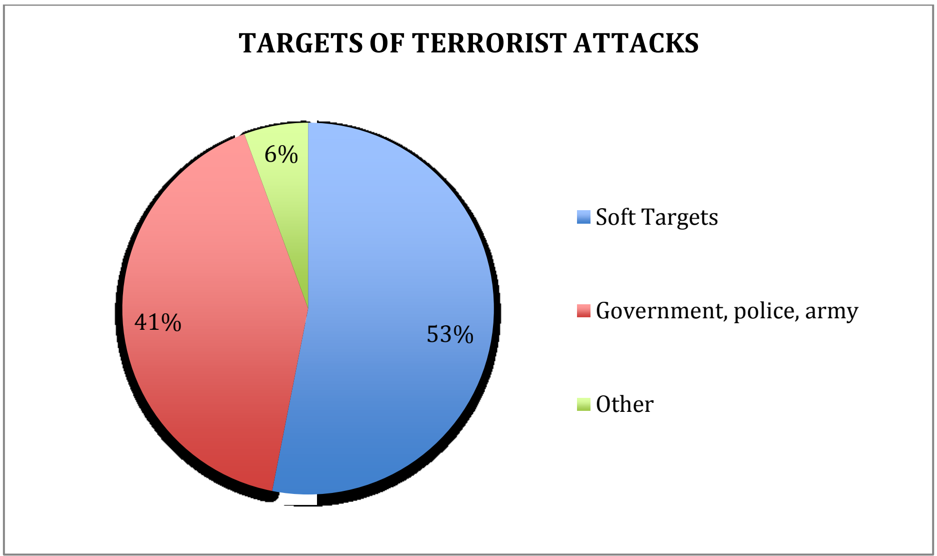
Attacks against transportation networks and vehicles can not only affect great amounts of people but also paralyze transport infrastructure, which multiplies their impact on the society.

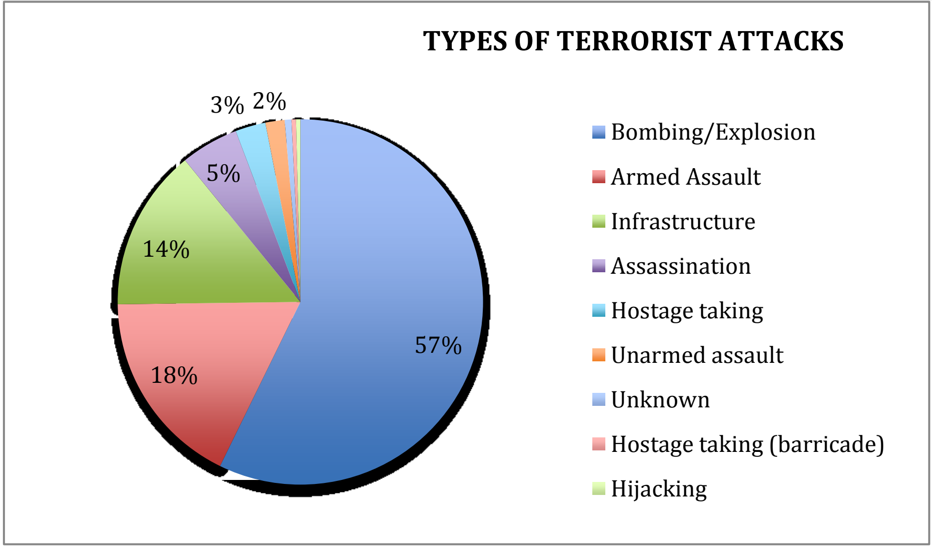
Terrorist threats and the soft targets

Soft targets face a wide scale of threats of various types by individuals or groups driven by a variety of motives. In order to create an efficient security methodology, it is necessary to deal with the threats systematically and to consider the available security measures with regard to the attackers' *modus operandi*. For the purpose of this Guideline, which should be universally applicable and yet maintain sufficient efficiency, we have decided to base our considerations on the experience with terrorist attacks. Anti-terrorist strategies are thoroughly tried and tested and take multiple factors into account. That makes them relevant to majority of possible attacks against soft targets. The current trend of terrorist attacks is to target public premises with weak security, while symbolic links to a specific religion or nationality seem to lose their former importance[3]. Therefore, protection of soft targets has been brought into greater attention and represents a security challenge of its own. Specific threats which deal with principles that differ from those applicable to terrorist attacks will be dealt with separately.

[3] See: "*Changes in modus operandi of Islamic State terrorist attacks: Review held by experts from Member States and Europol on 29 November and 1 December 2015*". In: Europol [online]. The Hague: Europol Public Information, 2016 [cit. 2016-01-10]. https://www.europol.europa.eu/content/changes-modus-operandi-islamic-state-terrorist-attacks.

The following graphs show the terrorist attacks carried out in Europe in the period of 1998 – 2014. In total, there were 5297 attacks[4] which we have been ranked by target and modus operandi:





An analysis of past terrorist attacks has shown the following predominant forms of assaults. All these need to be considered and addressed if we want to design an efficient security system for protection of soft targets against terrorist attacks:

1. Bombing attack (except when the bomb is in a vehicle)
2. Suicide bombing attack
3. Bomb delivered by mail
4. Bomb in a parked vehicle
5. Car bomb driven by a suicide attacker running into the target

[4] The statistics is based on the data from Global Terrorism Database of The University of Maryland. The database includes both the completed and the attempted attacks.

6. Arson
7. Gun attack (pistol, machine gun etc. – active shooter)
8. Hostage and barricade situation
9. Attack with a cold weapon (knife)
10. Crowd attacking a soft target
11. Vehicle running into the target

Analysis of the previously accomplished or attempted terrorist attacks against soft targets has also highlighted several other important factors to keep in mind:

1. **The people present on the spot do not immediately realize that they are victims or witnesses of an assault**. The sound of shooting is often mistaken for the sound of fireworks (Charlie Hebdo 2015, Bombay 2008).

2. Typically, during the attack and immediately afterwards, while there is still very little reliable information about what is going on, **response and action is required despite the fact that the situation is still very unclear**. Delay caused by waiting for facts may have fatal consequences. Therefore, it is desirable to plan an immediate response not only in case of a full-blown terrorist attack (car bomb, shooting, explosion…) but also in case of secondary signs, such as the sound of firecrackers, the sound of explosion, panicking crowd etc. Uncertainty is an aspect which should be properly addressed in security response training.

3. **Attacks are often coordinated or simultaneous**. Attackers tend to hit several targets in a short time span. Therefore, it is necessary to be prepared (adopt adequate measures) for another attack, at least within the limits of the municipality (town, city) where the first attack(s) occurred.

4. **Terrorist attacks are predominantly bombing attacks**. Therefore, it is wise to train staff in detection of suspicious objects and to drill procedures in case such an object is identified.

5. **Attackers tend to choose the way with the least number of obstacles** – i. e. they stop at the first closed door. The door does not even have to meet any official security standards, the mere fact that it is closed usually makes the attackers move on. Security strategies should always keep the “closed door effect” in mind.

6. **Attackers often experience altered perception of reality**. They are often drugged, under the influence of strong suggestive manipulation of mind (so called brainwashing), on a suicide mission, or may be mentally ill. This makes

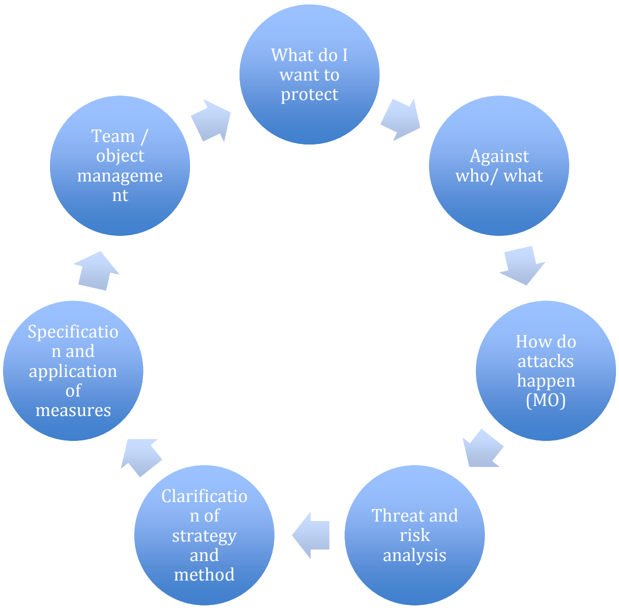
it much more difficult to predict the attackers’ behavior or to communicate or negotiate with them.

PRINCIPLES OF SOFT TARGETS PROTECTION

How to choose the right security measures

Soft targets comprise a huge and varied group of subjects. We have already outlined the main categories and the features which differentiate the soft targets from other targets but also one soft target category from another. We have also described the prevailing forms of terrorist attacks which provide a rationale for our choice of security measures. The data we have collected and analyzed help us to rationalize our security approach, to articulate the main principles of securing a particular target and to recommend specific steps to set up an efficient security system.

According to theory, these are the steps to be taken (or questions to be answered in the right sequence) before a functional security system can be set up:


What do I want to protect
Against who/ what
How do attacks happen (MO)
Threat and risk analysis
Clarification of strategy and method
Specification and application of measures
Team / object management

While creating a security system for a particular soft target (place or event), the first indispensable step is to **clarify what is to be protected**. Therefore, we start by defining the entities we value and do not wish to lose, and the harm that might be done. These usually includes the safety and lives of people, property, information, values or a good name. **This Guideline primarily addresses protection from violent assaults, i. e. the protection of lives and health. Nevertheless, the measures we discuss are also applicable to the disruption of public order, to some types of threat to property or to prevention of dangerous situations caused by technical accidents.**

In phase two, it is necessary to define **potential sources of danger/threat** against the protected entities. We identify particular enemy groups or categories of individuals with a conceivable motive to attack. In order to do so, we need to analyze previous attacks of similar nature and to consider potential sources of threat. It is necessary to keep in mind the specifics of the protected entity (presence of VIPs, attention of the media, high-risk timing of an event, explosives, resilience etc.).

Accurately defined **sources of threat** make it possible to forecast the **possible forms of attack**. These two aspects are the cornerstone on which we should build a security system for a particular soft target. Without a sound analysis of hostile interests and potential dangers, the security system will be inefficient and may lead to a waste of resources. Our Guideline is based on a systematic analysis of the threats posed to each particular soft target. Once the analysis is complete and the possible threats are defined, we can move on to select and implement adequate security measures.

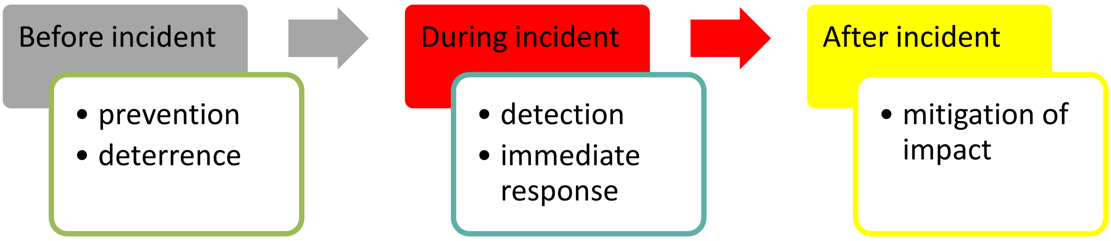
There are several methods of **analyzing threats and risks.** Above all, it is important to rank the threats by likelihood of occurrence (what is the probability that a threat will actually happen) and by seriousness of impact. Relevant data is fed to a security threat analysis (see Appendix 8) and that in turn generates a rating list of **major threats**. This list helps to set up the security system more accurately and to allot resources more effectively.

Knowing the major threats makes it possible to select the adequate **security measures** to be adopted. The next phase is implementation. The phase where technical equipment is installed and where customized security plans are created. The plans must define preventive measures as well as routine procedures and responses. In case an attack could not be prevented, attackers must be stopped at the earliest possible stage and the impact must be minimized.

This Guideline **deals explicitly with violent assaults**, i. e. with intentional acts by physical persons, threatening lives, health, freedom or dignity of the victims. Having said that, we should acknowledge that such attacks also lead to material and financial losses.

Time line: incidents and security measures

All incidents in question need to be handled in three phases. What can be done beforehand so as to reduce the likelihood of an incident, to minimize possible impact or to divert the attack altogether? What can be done during the attack? And finally, what can be done once the attack has occurred to mitigate its impact?



Before incident

- Take preventive measures to reduce the likelihood of an attack, to enhance the rapidity and intensity of the response, to reduce the seriousness of impact and to facilitate recovery
- Use tools to deter attackers and make them choose another target; create ways to divert the attack
- Use de-escalating communication to calm down a threatening situation and to minimize conflict

During incident

- Early detection of undesirable activity or infringement of restricted zones, ideally before the attack has begun.
- Immediate response of the guard force or other members of the security system, ideally following a pre-defined plan.

After incident

- The management deals with the situation as described in the pre-defined Coordination Plan, with clearly defined priorities for each post-incident phase
- Fast recovery of operation

Special attention should be paid to a very efficient method called DDRM (Deter – Detect – React – Mitigate impact). It is a tool designed to assess efficiency of security measures and solutions in the process of security planning. Having defined the possible threats which might attack the object in question we go item by item and suggest the best measures to deter, detect, react and mitigate impact. The measures that prove most efficient should be incorporated in the overall security solution. The final draft should be reviewed to ascertain that it provides guidance in all phases – before, during and after each of the incidents identified as a relevant threat.

Terrorist and other extreme attacks belong to the category of threats which a soft target can influence mainly in the phase before and after the attack. That is why maximum attention should be paid to the preventive measures which help detect the attack as soon as possible and to mitigate impact.

The immediate response, which might stop the attacker (physical protection), usually requires a professional team. Professionals are trained to eliminate the attackers using the right tactic and technical manner, while keeping the innocents out of trouble. Unfortunately, when a soft target is attacked, professional teams are usually not present. However, educated staff (or members of the public present on the spot) can play an important role in the phase of immediate response. They can call for help, stop the passers–by from entering the affected area, isolate people from the attacker by locking doors, warn others or even eliminate the attacker by themselves – if confrontation is the only and unavoidable means of self-defense.

Otherwise, if possible, it is always recommended to run or hide rather than fight (remember the American rule: run – hide – fight[5]).

All security solutions designed for soft targets must be:

- **fool-proof and efficient** because people's lives are at stake
- **creative** because the resources which the soft targets can deploy are usually limited,
- **flexible** because they must meet the needs of various environments and they must be applicable to attacks by various enemy groups, tactics and weapons.

[5] A didactical video is available at FBI website: www.fbi.gov/about-us/office-of-partner-engagement/active-shooter-incidents/run-hide-fight-video

CHOICE AND APPLICATION OF SECURITY COMPONENTS

The following chapter contains an outline of various security components divided into three basic categories:

1. security personnel
2. electronic devices
3. mechanical devices

Detailed classification of these components and their application can be found in many expert articles and books. With regard to securing soft targets, however, it seems more important to know how to fit the available components in a system. Electronic devices require a realistic vision, purposeful application and trained staff. No matter how advanced a revolving camera we install, it will bring little effect if we do not know who is going to operate it, what is to be looked for on the monitors and what should be done in case of a suspected threat. Similarly, mechanical devices, such as safety doors make little sense if incomers are checked by the door while out comers freely leave, leaving the access open periodically. And finally, regimen measures and procedures will work only if regularly updated and adjusted to the actual situations faced by your staff.

While looking for the right security components we should not base our decisions on top quality (the latest model, the most advanced version) but rather on purposefulness and compatibility with the other components of the system. Another critical factor to consider is who will be in charge of the new device and how is he or she going to be trained and monitored.

Security personnel

Guard force. Security guards can perform entrance checks and patrolling. They can also be in charge of the control room and the security technology placed inside. A well trained guard force is the most efficient security tool for deterrence, early detection, and immediate response as well as the mitigation of impact. Security guards can be employed by the institution in question or by a private security agency contracted by the institution. Security staff should abide by standardized procedures. The procedures must be tailored to the specifics of the given premises and revised on a regular basis. All routines must be described in detail and provide reliable guidance in case of less frequent situations. On the contrary, the procedures to be applied in case of security incidents need to be brief and must be reinforced with tactical training. The essential tool of a security guard is communication. That is why the training plan for staff should always include assertivity skills and crisis communication.

Other personnel. The term “other personnel“ applies to the employees who are not directly responsible for security but who participate in the organizational structure of the institution. Such employees can be receptionists, janitors, organizers, teachers, supervisors, ushers, volunteers or cleaners. A special role should be played by members of the management, who will also be trained to be able to coordinate recovery activities during the post-incident phase.

Electronic devices

Camera surveillance systems are used to monitor interior and exterior spaces, people and on-going activities. Camera surveillance systems can be attended continually by security guards or receptionists or can serve solely as a recording device for future use. If you cannot install cameras everywhere, it is advisable to monitor entrance area.

While determining the number of cameras to be installed it is wise to take into account the number of the staff in charge. It is not recommended to show more than 4 camera views on a 17 inch monitor. Cameras should be motion activated so dispatchers are alerted by the switch-on of the monitor. Movable cameras are less effective because in a bid to see everything you will probably end up seeing nothing at all.

Many camera surveillance systems have analytical functions, such as face detection or suspicious behavior detection. However, these analytical functions need to be operated and evaluated by qualified staff!

Security alarm systems serve primarily for detection of perimeter intrusion or unauthorized entry into a building or area. The systems are divided into perimeter, shield, spatial, object (perimetrické, plášťové, prostorové, předmětové) and offer a wide range of possible uses. For example: motion detectors, open door and window sensors, glass break sensors, fence climbing detectors etc. In all these devices, the alarm output may be local or remote – connected to a local switchboard, sent by SMS to a mobile device or sent out to a **Surveillance and Alarm Receiving Center**.

Surveillance and Alarm Receiving Center (DPPC) provides central dispatching services, including storage of selected data from secured premises, as well as remote surveillance and control.

Public address system is an extremely efficient tool of communication in case of an emergency. It is recommended to have two pre-recorded announcements – one for the evacuation of the building (in case of fire) and another for everybody to „stay put“ and „lock down“ .

X-ray scanners (further on referred to as „X-rays“) are used to detect weapons, bombs and explosives in baggage at the entrance check. X-ray check is performed simultaneously with a metal detection check. The check can be performed randomly. Efficient use of X-ray equipment requires well trained and regularly tested staff.

Metal detectors are available in two forms – as walk-through frames and as hand-held scanners. Both are used to check entering persons and detect metal weapons and metal parts in bombs. Metal detectors will of course not detect weapons and bombs made of other materials or explosives as such. Checks can be performed randomly. Efficient use of metal detectors requires trained staff.

Detectors of explosives (the so called “sniffers“) belong among the more recent and sophisticated security tools. They are demanding in terms of maintenance but relatively user-friendly. Sniffers are capable to detect a wider range of explosives than K-9 dogs trained to search for explosives. Sniffers are used mainly at entry checks, for example at random baggage checks or for the detection of suspicious objects or vehicles.

Entry and attendance control systems primarily provide data for the payroll office but at the same time can be used to make entry of unauthorized persons more difficult or to hinder unauthorized access within the building. Doors and walk-ins operating on chips, cards or biometric recognition can efficiently prevent criminal behavior and vandalism, however, it needs to be said that they do not provide sufficient protection in case of an active attack.

ID scanners are used for verification of identity documents presented at entrance check. Efficient use of an ID scanner requires well-trained staff.

Public emergency alerts (mobile applications, SMS portals) represent a very important means of early warning for people within a threatened area or organization. Personalized messages and a possibility to communicate with the dispatcher may significantly reduce tension and prevent people from entering dangerous zones etc.

Light (switched on by photo sensors) is an underestimated component of the security system. At minimum cost, it serves as one of the most efficient means of deterrence, especially when the light is switched on by a motion sensor.

Mechanical devices

Security doors of different grades of security ranking provide enhanced protection against forced entry and an overall resilience of the outer shield (plášťová ochrana) of the building. Security door can be bomb-resistant, bullet-resistant and extreme-intrusion-attempts resistant. In combination with access and attendance control technology it represents an efficient tool of preventing forced entry. It is important to keep in mind that the frame of a security door must be built-in to the walls, otherwise the door is less resistant to explosions. Ideally, the security door should be a part of the original construction plan. Replacement of frames can be rather complicated, especially in historical buildings.

Security windows which are bullet resistant, explosion resistant or breakage resistant in several grades of security ranking represent an efficient component of the shield protection of buildings. Same as the doors, window frames need to be firmly anchored in the walls, otherwise their resilience decreases. An alternative way to protect windows from various types of attacks, including explosions, are heavy curtains.

Fencing is a means of restricting access of unauthorized persons to protected premises. Fencing, especially if reinforced by security alarms and camera surveillance is an efficient tool for securing a perimeter by narrowing the access pathway.

Turnstiles are used to keep order and to authorize access at entrance and exit. For maximum effect, the rest of the perimeter or the outer shield of the building must be controlled. For security purposes, it should not be possible to climb over the turnstiles without the guards' notice. Turnstiles are recommended mainly to keep control at exits from large premises. The main advantage is that the people leaving the place cannot “hold the door open” for unauthorized incomers. Turnstiles are often fitted with an ID scanner.

Bollards, concrete medians and other mechanical barriers are used to prevent unauthorized parking (regimen measure) or access of a vehicle with a bomb (security measure). Attention should be paid to the material, anchoring and distance of the installed devices so that the bollards cannot be bypassed and that they cannot be easily destroyed or removed. Barriers installed in order to prevent access of vehicles must meet the parameters given by the estimated speed and weight of an attacking car.

SECURITY DIAGNOSTICS OF SOFT TARGETS

In the introductory sections, we have categorized soft targets by their function – schools, social events, shopping centers etc. However, a security solution should be designed separately for each individual entity and tailored not only to its function but mainly to its security specifics. The dominant criteria that should shape the final solution are: **desirability for a potential attacker** and **feasibility of security measures.**

Diagnostic factors to be considered are as follows:

- **Public accessibility**
- **Security personnel**
- **Many people concentrated in one place**
- **Presence of the police force**
- **Presence of the media**
- **Symbolic value of the target**

1. **Public accessibility.** Are we trying to secure an open-air event, a closed building or publicly accessible premises? In general, easily accessible open spaces are more attractive for attackers, especially if there is no way of checking attendants at the entrance. For security purposes it is important to control the perimeter, to narrow the access pathways and, if necessary, restrict entry to authorized personnel only.

2. **Security personnel.** Availability of security personnel has huge impact on the range of security measures we can deploy. Presence of security guards or “marshals“ by itself reduces the allure of the target.

3. **Many people concentrated in one place**. This is one of the two essential characteristics of soft targets and it is the reason why a place becomes a target in the first place. The more people, the greater the risk, even though the recent trend seems to suggest that there is a threshold beyond which further increase of people does not lead to greater risk. Anyway, the number and concentration of people gathering in a particular place in a particular period of time is a major factor which determines the security focus and security procedures.

4. **Presence of police force**. The police is an important means of deterrence and its presence reduces the desirability of a target. In soft targets, police are usually present only temporarily or locally to supervise maintenance of public order without much intervention. Permanent presence of police force hardens the target so that it is not a soft target any more.

5. **Presence of the media**. Terrorists and often also other types of attackers find presence of the media very attractive. Especially when important events are covered and broadcasted live by television.

6. **Symbolic value.** If terrorist or other violent groups attach symbolic value to a place or event, it becomes much more attractive as a target. For example Jewish, American or Roma content may increase likelihood of an attack. The soft targets of this kind should be prepared to face hostilities from the relevant groups, they should know the typical modus operandi of potential assaults and adjust their security plan to extremist threats.

Capability of self-protection is influenced by the following factors:

- **Organizational structure**
- **Resources and funds deployable on security**
- **Ability to identify one's own risks**

7. **Organizational structure.** This factor may not mean much to the attacker but it is a key feature with strong impact on the soft target's ability to articulate and implement security measures, to set up a feasible security plan and to launch security procedures when a threat is detected. For example when a place is owned or an organization is run by several entities as in the case of shopping centers or the monuments located in the Jewish quarter in Prague respectively security planning and response to threats must be coordinated. The organization should have a common security purpose, mutual consent on shared/delegated responsibility for security issues and a willingness to share both the workload and any costs that might arise.

8. **Resources and funds deployable on security.** Soft targets trying to put suitable security measures in place are influenced by their security budgets. Another factor linked to deployable resources is the post of a Security Manager, i. e. a person employed by the organization and responsible for all security issues.

9. **Ability to define one's risks**. Different entities possess a varying degree of ability to assess which activities and situations are risky, what the security should focus on, what is / isn‘t important and what can / cannot be handled without help from outside. This ability often depends on whether the organization has a Security Manager or another member of staff responsible for security and for communication with the police.

Using the above stated factors, every soft target can identify its strong and weak points, opportunities and threats (SWOT). The SWOT chart can be used when planning how to strengthen security in the future.

TEN ESSENTIAL RECOMMENDATION TO INCREASE RESILIENCE OF SOFT TARGETS

1. **Understand your security specifics**. Start by identifying what it is you want to secure and which of the activities you do or the people you deal with might make you desirable as a target. What are the high-risk times during the day, month or year? Who can you assign with security tasks? Which security solutions have proven successful? Specify what you want to focus on and the strengths and weaknesses of your defense.

2. **Be methodical.** Your security solution must be cost effective. Therefore, you must first clarify what kind of incidents need to be solved and only then determine which measures you want to adopt. Buying new gadgets is NOT your goal. Your goal is to be able to eliminate threats before, during and after an incident. For each security component already in place or considered clarify the purpose – what is it actually good for? Who is going to operate it? Who will train and supervise the operator?

3. **Engage local staff**. Local employees can play an important role in prevention, early detection of threats and mitigation of impact of security incidents. Even if you do not have security guards, assign the tasks and responsibilities to your employees, volunteers, assistants, "marshals" etc.

4. **Focus primarily on prevention and mitigation of impact.** Your task is NOT to eliminate the attacker but to do your maximum to prevent an attack, to detect threats as early as possible and to mitigate impact of security incidents. Elimination of the attacker should be left for the police or armed security force.

5. **Stick to standard procedures.** Set up your own plans and procedures for all relevant situations – checking visitors, checking documents, responding to suspicious situation etc. **Get ready for evacuation as well as invacuation**. It is not always best to evacuate people outside as in cases of fire. When the target seems to be under attack (shooting in front of the building or in the reception area, fighting inside the building, armed robbery etc.) it is safer to stay inside the building and lock down until the police have arrived. Set up your "lock down" procedures and if possible identify a suitable room which can serve as a lockable shelter – the so called "safe haven".

6. **Set up a coordination plan for your management**. The situation after a security incident is extremely stressful. It is necessary to make various decisions and it helps a lot if some of these measures have been taken

beforehand. Responsibilities for various areas need to be assigned to particular people and their actions need to be coordinated.

7. **Raise security awareness** of your staff and other people visiting your premises. Make sure to bring forward the topic of potential threats and to revise response procedures on a regular basis. Drill procedures from time to time.

8. **Set up cooperation with your local department of the Police CR and municipal police**, or with other units of the Integrated Rescue System (namely the Fire Squad or Health Care Rescue Squad). Offer to show them around your premises, discuss potential threats, share information about special events and consult your security plans for emergency situations.

9. **If you perform entry checks, don’t only look for weapons but also for harmful intentions**. Security frames and X-rays will only detect a weapon if operated by well-trained and regularly tested staff. Even if there is no weapon to be found, a motivated attacker will always find something weapon-like beyond the checkpoint. Apply methods for detection of suspicious behavior and security interviews to find out who is entering and whether s/he does not show suspicious signs.

10. **Take into consideration the surroundings of the soft target.** When securing soft targets we must often protect a whole area rather than an isolated site or organization. This is particularly true about soft targets located in close vicinity to each other or comprising a complex (for example a shopping gallery with an adjacent hotel).

RECOMMENDED COURSE OF ACTION

1. Understand your security specifics

To start with, identify the threats and dangers you may be facing. The best tool to use is a simple SWOT analysis which will help you identify your strong and weak points, opportunities and threats. The main factors to be included in your analysis are listed on page ….

It is very important to understand how the likelihood of a threat varies during a typical day. Attackers will choose a time when their attack would choose maximum damage. What time of day are the most people present? When do you hold events attended by even more people and perhaps journalists? What are the peak hours? When do people congregate in front of your building?

You should make a budget showing how much money can be allotted to security, which members of staff you can use and how much time can be spent.

2. A systematic approach to security development

As a matter of fact, the majority of soft targets do not have a Security Manager. With that in mind, we recommend using the existing workforce and the following protocols:

1. Designate an employee who will be responsible for the security agenda.
2. Carry out a soft target security analysis, including:
   a. Identification of threats (type of potential incidents) with specified place and time within the given site / event,
   b. Estimation of likelihood and impact of each specified incident (Threats and Risks Analysis – see attachment),
   c. Decisions as of which threats will be accepted, which will be delegated and which will be addressed.
3. Following the security analysis, determine the most suitable security measures. Which electronic and mechanical devices, what kind of security personnel and regimen measures will best serve to deter, detect, react or mitigate impact for each specified threat?
4. Finally, set up a plan for implementation of the measures you have chosen (security development plan) with a "roadmap" for e.g. 2 years.

3. Role of non-professional personnel

Only few soft targets employ their own security guards. The mere presence of security personnel does not guarantee that all important security tasks will be properly performed, and on the contrary, many security measures do not require specialized skills and can be carried out by any member of staff (if taught how).

All employees should be informed about the following:

- What are the specific risks related to a given site / event;
- How to identify a suspicious object, vehicle, person or delivery ;

- What to do in case of attack or other serious incident, in particular:
    - Who and how should be informed in case of suspicion or incident,
    - How to decide where to evacuate,
    - How to detect a suspicious delivery / mail,
    - How to react to a threat call.

In schools which have not installed a system of authorized access it is recommended to engage the teachers and the janitor and brief them with what to do in various standard situations, such as:

- Who will replace me at the entrance when I “have to“ leave because another duty is calling,
- What is the protocol if a suspicious person is waiting in front of the school,
- What is the protocol if a suspicious person tries to enter with a group of children,
- What is the protocol if somebody claims to be visiting the headmaster, a fellow teacher or other member of staff,
- What is the protocol if a parent insists that s/he must accompany his/her child to the changing room / classroom,
- What is the protocol if students report a suspicious person / baggage / vehicle,
- What is the protocol if a person claims to be authorized to pick up a child but his/her name is not on the authorization list or the staff does not know him /her.

The issues listed above apply (with modifications) to other kinds of soft targets as well.

At social events, it is possible to engage volunteers in safety protocols even when they are hired to help with various other tasks.

Non-professional personnel and prevention

The main asset of local staff is their knowledge of the local environment. It provides the best prerequisite for detection of persons or objects which are not a part of the routine and might be dangerous. Lack of such ability to detect suspicious persons and objects is the major weakness of security professionals who are occasionally hired for short-term jobs. They possess professional know-how but they do not understand the environment.

Non-professional personnel are present at the location and will be usually the first source of information about upcoming danger or the occurrence of a security incident.

To engage the non-professional personnel it is necessary to explain what role they might be expected to play. They need to understand what they should be watching for and the protocols if they see suspicious behavior or events. It is recommended to hold regular security trainings and briefings before relevant events and to outline emergency contacts.

Non-professional personnel and immediate response

Reacting to security incidents of a violent nature are extremely difficult because they present extreme stress load. People have to react without any support or guidance and they are often required to act against their natural instincts: run – freeze – fight.

Nevertheless, it is advisable to "inoculate" the lay personnel with a first reaction or the initial direction they should take in case of a security incident. For each building, place or event, you should make a list of potential security incidents with one the following reactions:

1. Listen and calm down conflict!
2. Warn others and prevent access to the incident
3. Run!
4. Hide and lock down!
5. Fight!

A protocol of recommended immediate responses to be applied by local staff until a professional, a superior or the police force have arrived might look as follows:

SITUATION	REACTION
Panic or unspecified incident	**1.** Don't try to find out what has happened, ACT! **2.** Where is it safer? Outside or inside? **3.** Navigate other people to safety. **4.** Keep in touch, contact your superior.
Verbal conflict	**1.** Calm them down! Show interest in solving the situation. **2.** Inform security personnel.
Physical conflict of low intensity (e.g. a fight)	**1.** Inform security guards or the police 158. **2.** Try to isolate others, reduce number of people under threat. **3.** Think twice before engaging in the conflict, consider your capability of fighting for yourself or another person **4.** If you are under threat and it is not possible to run or hide, then fight!
Technical accident (collapse of supporting construction etc.)	**1.** Mind your own safety, the situation may continue to worsen. **2.** Inform security personnel. **3.** Warn others and navigate them to safety.
Physical conflict armed	**1.** Run and warn others! **2.** If you cannot run, hide, lie down and lock down! **3.** If there is no other possibility, then fight!
Threat of explosion	**1.** Take cover! Stick to the rule: wall is good, glass is bad. **2.** Warn others.

A popular saying in security circles goes: *the most difficult decision is to make a decision.* Even experienced teams may find it difficult to launch a crisis procedure with far reaching consequences. Attacks are extremely stressful and people who have not undergone special training cannot be expected to react in a prepared manner. Professional reaction requires tactic drilling under stress. However, clearly defined basic instructions adjusted to a particular event may help reduce the risk of unexpected reactions.

Non-professional personnel and mitigation of impact after an incident

When an extraordinary situation such as a violent assault occurs, the immediate response and mitigation of impact will probably be assisted by the Police force, Fire Squad and Health Care Rescue Teams operating within the Integrated Rescue System (IRS).

Nevertheless, the owner/administrator of the affected soft target or the organizer of the affected event will have to:

1) manage the situation before the Integrated Rescue System (IRS) teams arrive (which may take up to 15 minutes depending on the location)
2) handle internal communication within the organization and other tasks beyond the IRS responsibilities.

Before the arrival of IRS teams, the local staff can help:

1. isolate the affected area and prevent more people from entering the dangerous perimeter.
2. provide preliminary First Aid.
3. navigate people to safety – inside or outside as required by the situation.
4. “re-organize“ event – for example when an event is held on a large area (e.g. Marathon race) and some of the participants may not know that a security incident has occurred, the organizers can divert (re-route) everybody into a selected safe area and provide them with information about a safety issue.

The more the people feel that an authority has the situation under control, the calmer they are and the less likely panic erupts. Authority can be effectively enhanced e.g. by wearing reflexive vests – which do not have to be carried around by the security personnel all the time but can be stored in pre-specified places (on each floor, in each conference room, at each route section etc.) in case of evacuation etc.

Once the IRS teams have arrived, the situation usually calms down and the local staff can help:

1. Navigate Rescue Teams, using the knowledge of local environment
2. Help maintain limited / restricted access to the affected area
3. Redirect all inquiries of the media, the people at the location and concerned families to the headquarters and/or a designated spokesperson

4. Keep record and evidence of the injured
5. Keep evidence and take care of unattended personal belongings, things left behind in changing rooms etc.

The owner of a building or organizer of an event needs to know the state of his/her staff. Is everybody alright? Has the ambulance taken people to the hospital? How many? Who are they? Which hospital? To keep things under control it is necessary to:

1. have a list of staff including contacts and assign a person who will check on each person's state and keep record of everybody's whereabouts.
2. educate the staff by means of security training / briefing. Let everybody know who their contact person is, save the contact telephone number and agree on a meeting point in case the telephone contact cannot be used.

Training of non-professional personnel
Training needs to be adjusted to each particular organization or event. In general, this is what you should always do to make your staff ready:

1. Let everybody know what security incidents might possibly occur:
    a. The situations need to be presented in such a way that all participants understand and can envision what might happen and know the protocols if an incident occurs.
    b. The staff should know that the organizer is doing maximum to secure the event but that despite all efforts, certain unexpected situations may arise.
2. Highlight the importance of staff in the security system:
    a. Everybody, including laypersons, can help.
    b. The staff should know that they will be perceived as an authority associated with capability and trustworthiness.
    c. The staff should be aware of their special mandate and local knowledge which make them indispensable.
3. Share examples of what the staff can do for prevention, immediate response and recovery:
    a. Prevention: regulating access, detection of conflict situations, technical problems, unattended baggage, suspicious persons, crowds (tlačenice) etc.
    b. Immediate response: navigating, giving information, running away, taking cover, calling help etc.
    c. Recovery: providing first aid, helping the IRS teams, navigating other people to safety, supplying info to the management
4. Make sure everybody knows who to inform in case of a security incident.
5. Revise / practice procedures for the most likely security incidents.

4. Measures of prevention and mitigation of impact

Serious assaults are hard to stop once they have occurred. However, the attackers can be deterred and an attack can be diverted by noticeable security measures or by creating a reputation of your “secureness“ in the media. Even if you haven’t managed to discourage the attackers and they intend to strike, you can detect signs of an attack in process when the attackers collect information about you. The most efficient active way of preventing an attack is an early identification of suspicious persons, objects, vehicles or deliveries.

The **method of how to detect suspicious behavior,** which used to be applied exclusively at airport checks, has spread into public environment. It is widely used and training is easily available.

How to detect suspicious behavior

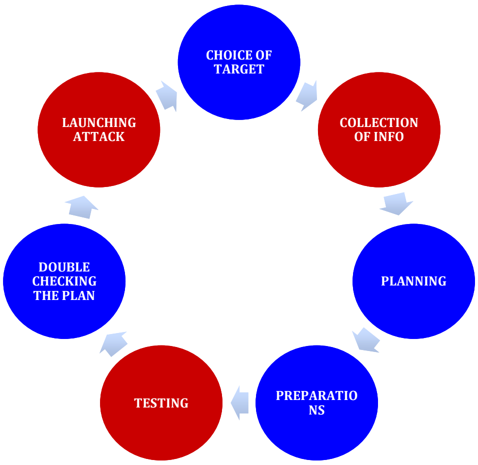
The method of detecting suspicious behavior is a part of the so called pro-active security approach. The idea is that the security system should not wait for an attack to happen but do its best to identify suspicious activity before an attack so that the threat can be eliminated or that the system can get ready and respond with maximum effect and speed.

The method is based on an active search for suspicious signs in the protected area and, if possible, its surroundings. This is not possible without a good knowledge of local routine and of the people who are a part of the scene – their behavior, appearance, the documents they bear, communication manner or other applicable characteristics. Relevant signs have to be generated for each environment independently with regard to its specifics. Above all, it is necessary to identify what is “normal“ for the place. The best tool to use is a “contextual analysis“. If a terrorist attack seems to be a possible threat, a contextual analysis is complemented simultaneously with an analysis of the attackers’ behavior. We try to model different types of incidents in the given environment and take note of everything that the attacker has to do to achieve his/her goal (such as to place a bomb in a desirable place, to stab the CEO on his/her way to the office, to collect information about the target etc.). Knowing what to expect from an attacker helps identify the suspicious signs which a) contrast with the routine and b) bear resemblance to the anticipated behavior before an attack.

Detection of suspicious behavior can be done using various methods. The most elementary form is a simple reflection of the types of people present in the given area, their characteristic behavior and appearance. In a school the applicable categories could be: the staff, students, students’ parents, suppliers and service companies, members of a basketball team (private rental in the afternoons) and so on. In shopping centers the categories might be: vendors in the retail units, employees of the center, cleaning and security, homeless people, pensioners and mothers with baby prams (morning), corporate employees who work in nearby offices (lunch time), kids and teenagers (afternoon), cinema goers (evening) and so on. Each of these categories has its typical behavior – entry and exit places, routes, degree of familiarity with the place (do they know their way or do they fumble around?), use of toilets, presence and type of baggage, means of authorization at entry (if any) and so on.

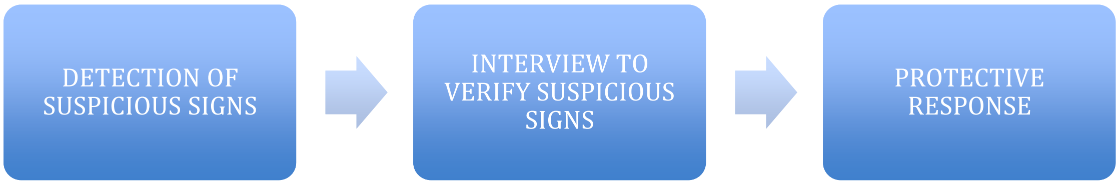
The objective is to give the security staff a clear idea of what is “normal“ so that they can identify deviations and abnormalities. Qualified staff should then be able to assess whether the identified deviations can be signs (symptoms) of undesirable activities going on. However, even non-professional personnel should be aware of the need to look out for suspicious or unusual signs because the knowledge of local environment is an absolutely crucial prerequisite for successful application of this security method. Long term experience and daily presence at a location cannot be replaced by any professional skills.

Sophisticated security systems, especially those which face the threat of terrorist attacks, have developed a more detailed classification of suspicious persons according to the phase of preparation for an attack. Analysis of previous attacks shows that the preparation can take up to several months. During the preparatory period, attackers collect information about potential targets in order to identify the most suitable one. Information on a location is researched on the Internet but some data cannot be obtained in any other way than by observation and sometimes also by provocation of the security systems of the targeted place.



Detection of suspicious behavior in areas threatened by terrorism is focused on early detection of the attackers’ collecting information, testing of the security system, and presence at the location before launching the attack. In areas where a terrorist attack (preceded by a long preparatory phase) is not considered relevant, soft targets should focus on the signs of an attack under way and on their readiness to respond.

Detection of suspicious signs is only one of two steps necessary for efficient protection. The first step is detection and the second is adequate response. The response varies according to the abilities and possibilities of each security system but also according to the phase of attack suggested by the detected signs. A simple protocol for detecting suspicious signs may look like this:


DETECTION OF SUSPICIOUS SIGNS
INTERVIEW TO VERIFY SUSPICIOUS SIGNS
PROTECTIVE RESPONSE

A different response is required when the collection of information is suspected than when there are signs of an active shooter. In most cases, however, the best thing to do when a suspicious person is identified is to verify suspicious signs (usually by means of communication with the suspect) so as to confirm or negate the suspicion. It should be taken into account that many people stand out from the local routine for various reasons. Existence of a suspicious sign in itself does not mean that the person is an attacker or a terrorist. All it means is that you should observe the person and watch for the signs of escalating threats.

Interviews carried out by security teams follow a strict protocol. When suspicious signs cannot be negated or when the signs seem to suggest presence of an active shooter who is intending to strike, it is necessary to launch a preventive response in order to mitigate impact of a potentially upcoming attack. Such a response may be closing the front door, holding up people who are about to leave the building etc.

6. Standardization of security procedures

Commonly enough, owners of soft targets underestimate the need to set up guidelines in case of standard security situations, believing that “common sense“ will help the staff handle everything. In fact, experience shows that without set protocols even minor incidents often lead to confusion, chaos and the inability to react adequately under pressure.

It is highly recommendable to define and write down the following procedures (if applicable to the subject in question):

- Restricted access to premises: form of authorization and control
- Restricted access for vehicles: form of authorization and control of vehicles
- Response to threat call or annoying call
- Response to identification of a suspicious object
- Response in case of verbal conflict / assault
- Response in case of aggressive incident (assault or threat without a weapon, without intention to kill)
- Response in case of a deadly assault or threat
- Procedure “lock down“ (closing oneself in a room)
- Plan of educating and training staff in security procedures

- Customized management Coordination Plan for mitigation of impact after an incident

All the above mentioned procedures can be set up by non-professional personnel with a good knowledge of the secured place. The process of setting up the guidelines helps clarify / solve many factors which may come up in case of a security incident and for which there would be no time once an incident has occurred.

Get ready for both evacuation and invacuation. It is not always best to evacuate in line with fire regulations, i.e. out of the building. When you are threatened by other danger (e.g. shooting in front of the building or in the reception area) it is often wiser to stay inside the building. Set up a "lock down" procedure and consider, if applicable, procedure "safe haven"[6].

"Lock down" is a procedure applied in schools and office buildings when it is not possible to leave the affected site / building and it is safer to hide inside. Typically, a "lock down" is applied in cases of armed attacks. The procedure includes a warning method – by public address system, shouting, normal sms, message shown on the display of mobile phone etc.

Launching "**lock down**" procedure:

1. The goal is to leave publicly accessible spaces and find shelter in the nearest lockable room
2. Once inside, lock yourself or block the door
    a. If possible, blind all openings, do not stay near the windows
    b. Hide by the door, under the table etc. ("duck and cover")
    c. Keep quiet, set your mobile to silent mode
3. Wait for instructions of the police or security personnel – until then, do not leave the room

7. Management Coordination Plan

[6] The „**safe haven**" is a pre-prepared, reinforced and equipped shelter which provides the best possible protection within the limits of the attacked site. The safe haven procedure is used mainly in cases of bombing and missile threats, provided that it is not too risky to move around the building. „Safe haven" is not applicable in cases of active shooters when people should not risk meeting the attackers in the corridors. Setting up a safe haven requires more advanced training and experience, which many subjects do not possess. If that is the case, it is recommended to use the plain „lock down" procedure.

A „safe haven" can be improvized in almost any building. Ideally, the room should be without windows, with strong walls and a lockable door. The people hiding in the safe haven may need to spend several hours locked inside, until a police rescue team arrives. Therefore, the shelter should be equipped with an adequate amount of water, blankets, medical kit, grape sugar, a torch, and possibly also a radio transmitter tuned to the security frequency of the building. If the room has windows or glass cabinets, it is recommended to cover them with heavy curtains to protect people from shattered glass.

The management Coordination Plan is a document which defines priority tasks for separate phases of a security incident and assigns people who will be responsible for each task. The purpose of this document is to help the management reduce stress, make decisions, define responsibilities and minimize chaos. Besides, the plan contains all materials and documents which are necessary during a security incident.

Different events require their own Coordination Plans. Different types of threats mean that the Organizer must be ready for different situations, with different people in charge and different priorities for each separate phase of the incident. A lot depends on the qualifications and experience of the Organizers but in general it is often true that "less is more". A few clearly defined binding rules are usually better than a set of sophisticated professional propositions which do not work. If a document contains too many protocols, it becomes more difficult to act upon them under stress.

The coordination team includes primarily the members of management but it is crucial to ensure that in case of a security incident everybody will be available and that other responsibilities will not interfere with the coordination work.

The plan should be well structured and contain answers to the following questions:

1. What kind of event requires activation of an emergency plan?
2. Who is in the coordination team?
3. What are the responsibilities of each member of the team?
4. Where is the coordination team going to work?
5. Where should each team member go once they have learnt about a security incident?
6. Are other activities threatened? Who in the management will be responsible for them?
7. How shall I know who has been injured and where they were taken?
8. Who will be the liaison officer with the IRS teams?
9. Who will check up and keep records of the staff?
10. Who is authorized to communicate with the media / key partners etc.?
11. Who will deal with inquiries from families, friends etc.?
12. Other

Tasks for management in case of a security incident should be listed chronologically and ranked by phase. Each phase of a security incident has its priority tasks and each member of the team should know where exactly s/he should be and what s/he is responsible for. The basic phases and tasks are defined as follows:

TIMELINE of PRIORITIES				
	PHASE 1	**PHASE 2**	**PHASE 3**	**PHASE 4**
TIME	**0-15min**	**15min – 3 hours**	**3 – 6 hours**	**Later**
PRIORITIES	1. React on the affected spot 2. Inform the IRS 3. First Aid	1. Coordinate your presence with IRS teams on the spot 2. Protect other activities 3. Adopt measures in	1. Stabilize activity of the Coordination Team (logistics, facilities) 2. Keep record of injuries	1. What happens tomorrow? 2. Refresh the Coordination Team

		accordance with the Coordination Plan	3. Keep info updated	3. More efficient internal communication
TASKS	- Isolate the incident and prevent further spreading - Help victims on the spot - Activate the Coordination Team	- Cooperate with IRS teams - Collect information about what is happening - Supply info into the organization (internal) - Secure future and remote activities	- Brief the Team regularly - Improve accuracy and distribution (multichannel) of external and internal information	- Psychological support - Rotation of the Coordination Team members

How to set up a management Coordination Plan

1. **Nominate the Coordination Team and select a Coordination Center**

   The first step is to assign the members of the **Coordination Team** who will be responsible for managing the organization immediately after a security incident. The Coordination Team will have to bear the responsibilities and deal with the consequences arising from a potential security incident. Its agenda must correspond with the capacities and resources of the given organization. Another important decision is where to create a **Coordination Center**, i.e. the place where the Team is going to meet. Find a suitable location and define a set-up procedure. You must know how to equip the Center and what documents will be needed. The Center should be closed, providing sufficient privacy for work, with restricted access of other members of staff. In case of a terrorist attack the Center should be located outside the affected area.

2. **Match management priorities with the separate phases of an incident**

   Time is one of the main factors to consider while setting up a Coordination Plan. Timing in an incident is paramount as the situation and the needs of victims change dramatically. The Management Plan highlights priorities and helps allocate the available funds and resources as efficiently as possible.

3. **Specify tasks for each member of the Coordination Team in each phase**

   Assign tasks to the Coordination Team members (communication with parents, establishing contact with the hospital, writing a press release etc.) Specify tasks as well as the tools to be used by each of the Team members. All tasks must be worded with maximum clarity and practicality so that they can be performed by non-professionals.

4. **Dissimulate emergency, train procedures, verify functionality**

   Coordination Plan is always customized. To verify whether the Plan works well in the given context it is recommended to **dissimulate emergency and to test the readiness of staff by means of emergency drills.**

8. Raising security awareness

In general, it is recommended to **brief the staff about potential threats** and to **revise basic security procedures** at least once a year.

Take good notice of conflict and suspicious situations, security incidents, technical accidents relevant to security etc. Keep a thorough record and statistics of such occurrences even if they may seem banal or commonplace.

Encourage your staff, colleagues or even neighbors to report suspicious activities, such as strangers soliciting information about the area etc. If anybody notices strange or suspicious occurrences, they should inform the security guards or the police at 158.

Recommendations:

1) Once a year hold a **security training focused on prevention and procedures to be applied in case of a security incident.** The agenda may include security procedures, drilling, crisis communication, self-defense etc.
2) Once a year hold a **training of management** focused on coordination of activities immediately after a security incident. The training is more effective when combined with an obligatory fire-drill.
3) Address security issues in **your corporate periodicals, mobile applications etc.** in order to make your staff and visitors aware of security risks and prevention .

When you organize big cultural or sports events, provide **security briefing for volunteers and organizers**.

9. Cooperation with the Integrated Rescue System (IRS)

Cooperation with the various sections of the National Integrated Rescue System – i.e. the Police CR, Municipal Police departments, Fire Squad, Health Care Rescue Squad etc. can help you increase your security, set up a security plan and prevent security incidents.

It is recommendable to establish contact with the IRS, to engage IRS teams in organization of events and to have your premises assessed by IRS experts. Besides, it is wise to inform the Police CR about special events and consult the measures to be adopted in case of security incidents. Contact your local / regional department of the Police CR, the Municipal Police or the Prevention and Information Department. Share relevant information (such as building plans) with the operational headquarters of the local Emergency Office.

10. Consistent authorization of access and focus on detection of harmful intentions

Security checks at the entrance of buildings or premises are a common security feature but regrettably the effectivity of such checks is often impaired by inconsistency or poor execution. Moreover, in soft targets, such security checks are not possible because a soft target is often by definition publicly accessible or located in an open space.

If it is possible to control the perimeter and introduce entrance checks, there are three possible levels of control:

1. Authorization of persons
2. Authorization of persons and detection of undesirable objects
3. Authorization of persons, detection of undesirable objects and detection of harmful intentions

To make the authorization measures effective it is necessary to control the whole perimeter at all working time. Consistent authorization means that every person entering the premises must be approved by a pre-determined protocol. Authorization can be carried out by a technical device (e.g. a scanner, cameras, video telephone etc.) or by means of physical identification by a competent member of staff.

Personal checks constitute a higher level of control. Security frames and X-rays cannot detect weapons by themselves. They must be operated by well trained and regularly tested security personnel. However, an attacker can get hold of various objects beyond the check point and use them as weapons. Therefore, it is best to apply a combination of checks focused not only on detection of undesirable objects but also on suspicious behavior and harmful intention. The latter is assessed by means of a **security interview performed by a qualified member of staff.**

Get to know your surroundings and cooperate with other soft targets

This recommendation is crucial in creating a purposeful security system. Attacks against soft targets are often coordinated or simultaneous and the attackers often strike against several subjects in a row. It is quite common that the assault takes place in front of buildings, without the attackers going inside.[7] This should be kept in mind when assessing vulnerability and introducing security measures – the attack often occurs outside the secured perimeter.

[7] This is why **long queues before security checks at entrances expose people to high risk** and it is often discutable whether this risk is worth the benefit of preventing potential attackers from entering the building. Look for the answer in your analysis of threats: what is the most desirable target for your potential attackers? The site or the people? And what is the most likely modus operandi?

The security management should know whether they are protecting primarily the building or the people in it (which is typical for soft targets) and to what distance an attack outside would impact on the secured organization, its wellbeing and its operation.

The area to consider is often much larger than just the immediate surroundings of the secured site. It can be a city or a whole region. That is why it is recommended to establish and encourage cooperation among soft targets (in a given area) and work together to set up measures beneficial for all participants. Examples of such cooperation can be sharing of information, mutual warnings in case of security incidents, sharing of a Coordination Center (see above), joint security drills, training of procedures, and the sharing of security costs etc.

APPENDIXES

Appendix 1 – What to do in case of a security incident: general recommendations

1. Call for help (tel. 158) – ASAP! Do not stay alone.
2. If you suspect occurrence of a serious assault or other incident, act immediately, do not hesitate, do not wait for more information.
3. If the police or security give you a warning with a recommendation to evacuate people, act immediately.
4. Be prepared to work under extreme pressure. If necessary, be ready to take extreme and creative measures – especially when it comes to evacuation. Do not let the rules limit you.
5. The elementary rule for all security incidents is: **get the people out of trouble.**
6. When you need to take cover from an explosion, remember that „wall is good, glass is bad“[8].
7. Don't let your imagination go wild, don't speculate about other possible threats – it will paralyze you. Act upon the situation you can actually see![9]
8. The place to which you evacuate people must be safer than the place from which you evacuate. Ask yourself: Is it safer inside or outside?
9. Communicate, speak loudly, say what you do.
10. Every time you evacuate, get the people at least out of the sight of the problem.

[8] After explosions, most damage is caused by secondary fragments, especially from shattered glass. A bombing attack often affects all windowshields in the building.

[9] The rule „do not let your imagination go wild“ applies to the situation when people facing an attack start imagining incidents that might be under way at other places (parallel multiple attack), trying to think of a solution for all. Experience shows that straightforward reactions to the situation in one's immediate vicinity are most effective. Speculations are a waste of time.

Appendix 2 – Recommended procedure in case of a threat call

In case you receive a threat call:

1. Write everything down in maximum detail.
2. If your telephone displays the calling number, write it down.
3. Never hang up! Try to make the calling person hold the line, ask questions and write down the answers.
4. When the call is over, report it to your security service.
5. Did the caller seem serious about his/her threats? Did s/he seem familiar with the suggested target? Was the threat specific? If the answers are yes, launch your evacuation procedure.
6. Inform the police at 158.
7. Assist the police and the IRS teams. Supply information, prevent access to the affected location etc.

Appendix 3 – Recommended procedure in case of a suspicious object

When the object:

- does not fit in with the local routine,
- is left unattended and the owner is not in sight,
- is large enough and placed in such a place that its explosion would threaten peoples' lives.

Act in line with the following protocol:

1. Inform the security staff.
2. Make sure that nobody touches the object or comes close to it.
3. Try to identify the owner. Check the people around. Use your corporate public address system.
4. If you do not know the owner, prevent people from coming close to the object. Evacuate (away from the object).
5. Inform the police.
6. Take a photograph.

Appendix 4 – Recommended procedure in case of a suspicious vehicle

If it is obvious that the vehicle is a “car bomb“:

1. Immediately evacuate away from the vehicle. Direct people to take cover behind walls. The more walls between the vehicle and the evacuated people, the better.
2. Engage security staff in the evacuation process.
3. Inform the police.

If the vehicle seems suspicious:

1. Do not touch, open or move the vehicle.
2. Inform security staff.
3. Do not focus on the driver but on the vehicle!
4. Try to identify the owner. Check the people around. Use the corporate public address system.
5. Inform the police.
6. Take a photograph (with a visible number plate if possible).

Appendix 5 – Recommended procedure in case of suspicious delivery

Suspicious parcels delivered by mail can by identified by the following signs:

- The sender is unfamiliar or unspecified.
- Your address is not 100% accurately written.
- The delivery was not expected.
- The parcel is uneven or knobby.
- The parcel is uncommonly large or padded.
- The wrapping seems oily and smells weird.
- The parcel has too many post stamps.

1. NEVER OPEN a suspicious letter / parcel!
2. Handle the suspicious delivery carefully and place it in a small closed room. The risk of activating a bomb by moving it is smaller than the damage that would surely be caused by an explosion in a crowded place.
3. Do not use radio transmitters in the vicinity of the object (mobile phones, walkie-talkies).
4. Inform your security staff.
5. Inform the police.
6. Take a photograph.

Appendix 6 – How to report dangerous situations to the IRS operator over the telephone

When talking to the Integrated Rescue System operator over the telephone, remember the following:

1. State your full name.
2. State your position in the company.
3. State the place from which you are calling.
4. Describe what has happened.
5. Describe the situation now.
6. Specify if there are injured people.
7. Specify your needs.
8. Do not hang up first.
9. In the next few minutes do not make any phone calls so that the operator can call you back.

Appendix 8 - Examples of assaults against different types of soft targets:

Schools

- Žďár nad Sázavou, Czech Republic, 2014. 1 casualty, MO: hostages, knife attack
- Brindisi, Italy, 2012. 1 casualty, 7 injured. MO: bombing in front of a school
- Toulouse, France, 2012. 4 casualties. MO: Shooting
- Winnenden, Germany, 2009. 15 casualties. MO: Shooting
- Beslan, Russia, 2004. 385 casualties, 1100 hostages. MO: Hostages, shooting
- Dunblane, Scotland, 1996. 15 casualties, 18 injured. MO: Shooting
- Vukovar, Croatia, 1991. 41 casualties, 0 injured. MO: Shooting

Religious (in the Czech Republic mainly Jewish) sites and places of worship

- Copenhagen, Denmark, 2015: 1 casualty, MO: Shooting nearby a synagogue
- Paris, France, 2015, 4 casualties, MO: Hostages and shooting in a kosher shop
- Brussels, Belgium, 2014. 4 casualties, MO: Shooting in a Jewish museum
- Dijon, France, 2014. 11 injured, MO: Car driving in a crowd
- Toulouse, France, 2012. 4 casualties, 1 injured, MO: Shooting in a Jewish school

Transportation

- Bologoye, Russia, train, 2009. 26 casualties, 100 injured. MO: Bombing attack
- Moscow, Russia, underground, 2010. 44 casualties, 88 injured. MO: Bombing attack
- London, England, underground, 2005. 56 casualties, 784 injured. MO: Bombing attack
- Madrid, Spain, train, 2004. 191 casualties, 1800 injured. MO: Bombing attack

Sports and cultural events

- Paris, France, 2015. 1 casualty at a football match. MO: Suicide bombing
- Copenhagen, Denmark, 2015. 1 casualty, 3 injured at a lecture on freedom of speech. MO: Shooting
- Boston, USA, 2013. 2 casualties, 132 injured. MO: Bombing attack

Shopping centers and restaurants

- Paris, France, 2015. 15 casualties and 10 injured. MO: Shooting from a car at a restaurant
- Uherský Brod, Czech Republic, 2015. 8 casualties. MO: Shooting
- Copenhagen, Denmark, 2015. 1 casualty. MO: Shooting
- Bombay, India, 2008. 10 casualties. MO: Shooting, granade, Leopold Cafe
- Tel Aviv, Israel, 2003. 3 casualties. MO: Suicide bombing, Mike’s place

Hotels

- Islamabad, Pakistan, 2008, 61 casualties, 200 injured. MO: suicide bombing
- Sharm el-Sheikh, Egypt, 2005, 91 casualties, 110 injured. MO: suicide bombing

- Taba, Egypt, 2004, 34 casualties, 159 injured. MO: car bomb
- Bombay, India, 2008, 68 casualties, 76 injured. MO: Shooting, bombing attack

Appendix 8 - Classification of threats through Risk Analysis

MODUS OPERANDI	PLACE OF ATTACK	TIME OF ATTACK	LIKELIHOOD				IMPACT				DEGREE OF THREAT
			Accessibility	Obstacles	Desirability	**Threat in total**	Damage to building	Threat to lives	Impact on community	Economical losses	
Attack with a knife	In front of the site	Daily working time									
Attack with a knife	In front of the site	Event for invited guests									
Shooting	In front of the site	Daily working time									
Bombing	Inside	Event for invited guests									
…											