The ways of assessing the security of organization information systems through SWOT analysis

Chapter · January 2011

DOI: 10.4018/978-1-61350-311-9

David Rehak

VŠB-Technical University of Ostrava

Chapter 7
The Ways of Assessing the Security of Organization Information Systems through SWOT Analysis

David Rehak
VSB – Technical University of Ostrava, Czech Republic

Monika Grasseova
University of Defence, Czech Republic

EXECUTIVE SUMMARY

The chapter is focused mainly on assessing the factors of the external environment in the area of security of information systems in the organization through SWOT analysis. At first the method is characterized from the viewpoint of its purpose and nature. The emphasis is laid on the principles of SWOT analysis, the possible use of methods and tools, and also the most common problems occurring during the implementation of the analysis. The recommended methodical procedure for the implementation of SWOT analysis is described in another part of the chapter with individual phases and particular activities, which are appropriate to be carried out within these phases. The main part of the chapter is focused on the ways of semi-quantitative assessment of threats to the area of information systems of the organization, while evaluating their risks, and the assessment of opportunities, while evaluating their benefits.

DOI: 10.4018/978-1-61350-311-9.ch007

Both cases include a detailed description of procedure leading to an objective outcome during the classification of identified threats and opportunities according to the set criteria.

INTRODUCTION

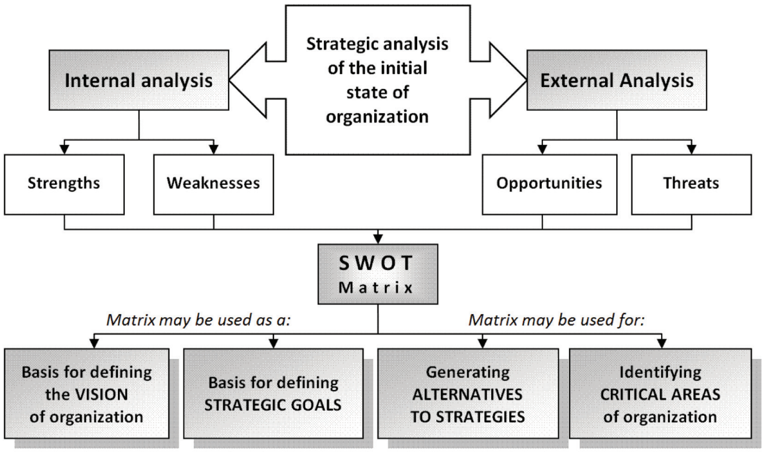
The assessment of identified threats and opportunities is a significant phase of SWOT analysis, which may fundamentally affect security of information systems of the organization. The most objective outcomes have to be achieved in this phase on the basis of which an optimal development of organization will be chosen. The assessment of threats and opportunities while evaluating their risks and benefits is one possibility of achieving such objectivity. An accurate assessment may also be achieved with the use of a multi-criterial assessment matrix. The chapter is aimed at clarifying the ways of assessing the identified threats and opportunities in the external analysis of the security of information systems in the organization within SWOT analysis.

SETTING THE SCENE

SWOT is an acronym for *Strengths*, *Weaknesses*, *Opportunities*, and *Threats*. Thus SWOT is the acronym for the internal strengths and weaknesses of organization and the opportunities and threats identified in the external environment of organization. SWOT analysis is one of the methods of strategic analysis of the initial state of an organization and/or its parts, generating the alternatives to strategies (see Figure 1) on the basis of internal analysis (strengths and weaknesses) and external analysis (opportunities and threats). A comprehensive SWOT analysis puts strengths and weaknesses of an organization or its parts against identified opportunities and threats ensuing from the surrounding environment and defines the position of the organization and/or its parts as a starting point for defining the strategies of further development.

The method was developed by Albert Humphrey, who led a research project in the 1960s-1970s at Stanford University. The project was financially supported by the 500 biggest corporations in the USA (Fortune 500) and its aim was to analyze shortcomings in the planning process of those corporations and develop a new system of change management for them. A team method for planning was called SOFT analysis and later revised as SWOT analysis.

Figure 1. The basic framework of SWOT analysis



SWOT analysis may be included among the most implemented analytical methods. Specialized literature usually includes only the outcome of the last phase of SWOT analysis, i.e. SWOT matrix (see Figure 2).

During SWOT analysis it is necessary to determine the purpose of its use, i.e. what the outcomes will be used for. SWOT analysis may be used for one or more of the following purposes:

- As a basis for defining the vision
- As a basis for defining the strategic goals

Figure 2. SWOT matrix

Internal Factors / External Factors	**Weaknesses (W)** 1. ………, 2. ………, 3. ………, etc.	**Strengths (S)** 1. ………, 2. ………, 3. ………, etc.
Opportunities (O) 1. ………, 2. ………, 3. ………, etc.	**WO strategy** **„Searching“** *Overcoming a weakness by taking advantage of opportunity*	**SO strategy** **„Taking advantage“** *Taking advantage of strength in favour of opportunity*
Threats (T) 1. ………, 2. ………, 3. ………, etc.	**WT strategy** **„Avoiding“** *Minimization of weakness and avoidance of threat*	**ST strategy** **„Confrontation“** *Taking advantage of strength to prevent threat*

- As a basis for the first generation of strategic alternatives
- For identifying critical areas.

Many organizations finish SWOT analysis with a detailed list of strengths, weaknesses, opportunities and threats. However, if the facts discovered are not used for the purposes as outlined above, the findings are basically useless. The question is, what the purpose of discovering the weaknesses of the organization is, e.g. in securing the information systems, if the organization does not work with such information any more. Many organizations carry out SWOT analysis just to claim it has been completed during the preparation of the information systems security crisis plan, for example. However, the fact that the plan does not reflect the outcomes of analysis is not considered. Therefore when implementing SWOT analysis it is necessary to consider the purpose of it and the further use of outcomes.

The analysis has not had a fixed methodological framework so far. General information on the SWOT analysis procedure is published in specialized literature rather than particular steps accompanying its practical implementation. Therefore one subchapter includes a recommended methodical procedure of implementing SWOT analysis. The procedure cannot be applied as a universal one, but it is necessary to amend it according to particular conditions, specifics of an organization and purpose of analysis.

The following principles are to be followed during SWOT analysis:

- The purpose has to be considered all the time during the analysis; procedures and outcomes cannot be mechanically applied to a different problem;
- It is necessary to focus on substantial facts; the statement of strategy is complicated in case of too much information. SWOT, as part of strategic analysis, should identify only "strategic" facts, i.e. long-term phenomena;
- Analysis has to be objective - it can be achieved with more people participating in its development;
- It is appropriate to use the system of assessing the power of factors, e.g. by using point scales.

The most often used methods and tools of SWOT analysis are as follows:

- The use of data from assessment and analytical reports and studies – it is usually the content analysis of elaborate documents, which include some type of analysis, either the analysis of the initial state or the prognosis of future development;

- The implementation of creative methods (e.g. brainstorming, panel discussion) and procedures based on professional forecasts made by competent entities;
- The implementation of appropriate forms, matrixes, graphs and point scales.

Characteristics of SWOT Analysis

SWOT is a type of strategic analysis of a company or an organization from the viewpoint of its strengths, weaknesses, opportunities, and threats. It provides data for stating the development directions and activities, company strategies and strategic goals. The analysis is based on the analysis and assessment of the current state of the organization (internal environment) and the current state of the surrounding environments of the organization (external environment).

The strengths and weaknesses of the organization are identified in the internal environment. Strengths and weaknesses define internal factors of effectiveness and ineffectiveness in all significant areas of the organization. The organization may be divided into the functional and procedural areas, or it may use a “7S” model (see part Preparation for SWOT analysis, step 2).

Opportunities and threats for an organization are identified in the external environment. Opportunities and threats define the effects of the external environment in all significant areas of the organization. The external environment affecting organizations in public and private sectors usually includes the following areas: P – political, E – economic, S – social, T – technological, L – legislative, E – environmental. The analysis of opportunities and threats may be carried out with the use of PESTLE analysis. The list of opportunities for a public sector organization may include, for example, available financial resources, public interest, interest of certain segments of society resulting in stimuli towards improved quality of services and international co-operation, and analysis of the political environment. The list of threats may include, for example, the outcomes of surveys of competitive environment within a selected segment, limited financial support provided to prepared projects from public resources and supranational organizations, lack of inventions and innovative processes in the area of interest, negative development processes of the national economy (macro and micro-processes of national economy), etc. Although the organization cannot affect external factors as much as internal ones, it should take appropriate measures to minimize them (in case of threats) or take advantage of them (in case of opportunities).

RECOMMENDED METHODICAL PROCEDURE FOR THE IMPLEMENTATION OF SWOT ANALYSIS

It is appropriate to start from the general principles for the implementation of SWOT analysis. There are four basic phases of SWOT analysis resulting from the lessons learned, regardless of whether it is the production sector or public administration: 1. Preparation for SWOT analysis; 2. Identification and assessment of strengths and weaknesses of the organization and/or its areas (SBU); 3. Identification and assessment of opportunities and threats from external environment; 4. Development of SWOT Matrix.

Individual phases of SWOT analysis are further divided into particular activities and steps. The described procedure of implementing each phase of SWOT analysis is based on proven practical experience and is not binding. As the method does not have a fixed methodological framework it is possible to amend the proposed procedure according to the needs and established practices of the organization and the level of strategy for which SWOT analysis is used.

Preparation for SWOT Analysis

Four steps are proposed to be followed in order, as follows: 1. Clear statement of the purpose of SWOT analysis; (2) Definition of the areas to be analyzed; 3. Establishment of analytical teams; 4. Standardization of work methodology and motivation of team members.

1. Clear Statement of the Purpose of SWOT Analysis

The purpose of SWOT analysis has to be stated, in case it has not already been stated by an employee who ordered the analysis.

2. Definition of the Areas to be Analyzed

In case SWOT analysis is applied to all of the organization, it is suitable to divide the organization into areas, which are then analyzed independently. The organization may be divided according to functional areas, procedural areas or according to McKinsey's "7S" framework. The division of the organization into functional areas may have the following structure:

- Management systems
- Organizational structures
- Information systems

- Culture of organization
- Human resources and their development
- Research and development, equipment
- Finance and economy.

The analysis of the following areas is carried out in case the organization is divided according to the process areas:

- Main processes
- Management processes
- Supporting processes.

The Mc Kinsey 7S model of internal analysis may be used in the analysis of organizations. SWOT analysis can then be used with focus on the following areas:

- Strategy
- Structure
- Management system
- Style of management
- Staff
- Skills
- Shared values.

If a strategic business unit (SBU) of the organization is analyzed it is also suitable to divide it into individual areas.

SWOT analysis may also be used for self-assessment of organization performance. The European Foundation for Quality Management (EFQM) Excellence Model is used for such an assessment in Europe. The model of Common Assessment Framework as the amended and simplified version of EFQM is used in the area of public administration. The self-assessment of organization performance is carried out on the basis of 9 criteria and SWOT analysis may be used as a basis for analyzing the individual criteria. Mainly internal analysis is used for identifying strengths and weaknesses, which are called the opportunities for improvement in this model. The Baldrige Criteria for Performance Excellence Framework is used in the USA and is similar to the above mentioned models.

The determined areas are then usually assessed independently with SWOT analysis. The SWOT analysis carried out within the organization security environment may assess independently the following areas: information systems, technological operations, work safety and health protection at work, etc.

3. Establishment of Analytical Teams

The analytical teams of experienced personnel identify and assess the factors affecting the analyzed areas. It is possible to establish a special team for each area, i.e. each area will be analyzed by a different team, which is the most knowledgeable and experienced in the given area.

4. Standardization of Work Methodology and Motivation of Team Members

All team members must agree on a particular procedure of SWOT analysis and adhere to it. It is suitable to determine the possibilities of collecting information and the methods to be used (or which are recommended to be used). The main motivation of the team members is the fact that they know the purpose of SWOT analysis and that their work will not be useless. The team members must have enough time and competencies in case they acquire certain information in discussion with the management of the organization.

Identification and Assessment of Strengths and Weaknesses

We propose two consecutive steps, which are described in more detail below: 1. Identification of strengths and weaknesses; 2. Assessment of strengths and weaknesses.

1. Identification of Strengths and Weaknesses

Strengths and weaknesses of the analyzed area of the organization may be identified in several ways, e.g. through the content analysis of initial data and the following implementation of creative methods, e.g. brainstorming, consultations, and guided discussions aimed at identifying or defining strengths and weaknesses of the analyzed area of the organization. It is necessary to record the strengths and weaknesses appropriately e.g. in a form, including the justification of the outcome. A sample form for the identification of weaknesses is shown in Table 1.

2. Assessment of Strengths and Weaknesses

The identification of strengths and weaknesses of the analyzed area is usually followed by determining their relevance from the viewpoint of their consequences for the analyzed area. The relevance of strengths and weaknesses is assessed separately using the method of pair comparison or the 100 points method.[1]

Table 1. Sample form for the identification of weaknesses

The analyzed area of organization: *e.g. Security of Organization Information System*	
WEAKNESSES	**WHY?** (justification - why we consider a particular factor to be a weakness)
A. Imperfect updating of information system	*Security gaps occur due to imperfect updating of information system. Malware may then infiltrate such information system.*
B. Infiltration of personnel	*It is unlikely that the company management detects personnel infiltrating the organization information system. Therefore the unauthorized use of data in the information system is quite extensive.*
C. Weak information infrastructure	*The data flows are programmed incorrectly in the information system. It can cause unintended and serious data leakage.*
D. Weak communication infrastructure	*The late updating of hardware may result in possible security errors, which enable malware to infiltrate the information system through unprotected ports.*

The procedure of determining relevance or the order of individual strengths and weaknesses through the method of pair comparison is as follows (see Table 2):

- Identified strengths/weaknesses are compared in pairs and their relevance is determined in relation to the analyzed area. The more important element of each pair is recorded in the table.
- The frequency of higher relevance is counted, i.e. the number of preferences in the pair comparison is counted. The values are summed both in lines and columns.
- The relevance – scale – of each strength/weakness is calculated by dividing the number of preferences of a particular strength/weakness with the total number of preferences (e.g. the relevance of A weakness is A = 2/6 = 0,33).

Table 2. The determining of relevance with the method of pair comparison of identified strengths and weaknesses

Process of determining the relevance	**a)**				**b)**	**c)**
Strength/Weakness	**A.**	**B.**	**C.**	**D.**	**Number of Preferences**	**Relevance**
A. Imperfect updating of information system		B	A	A	2	**0,33**
B. Infiltration of personnel			B	B	3	**0,5**
C. Weak information infrastructure				D	0	**0**
D. Weak communication infrastructure					1	**0,17**
Total					**6**	**1,0**

If the 100 points method is implemented, each team member divides 100 points among individual strengths. The more points are allocated to the given strength the more relevant it is considered to be in relation to the analyzed area. 100 points are similarly divided among weaknesses. Relevance may then be calculated as an arithmetic average from the individual assessments of analytical team members. If the assessment of any strength/weakness is considerably different among the team members, it is suitable to reach consensus rather than use the arithmetic average.

Once the strengths and weaknesses are identified they are arranged in the order of relevance according to the results of assessment. Thus two lists are made starting from No 1 as the most relevant strength/weakness to number X as the least relevant one with the least or no consequence for the analyzed area. The order of weaknesses is made on the basis of assessment outcomes (Table 2) and according to their importance as follows:

1. Infiltration of personnel
2. Imperfect updating of information system
3. Weak communication infrastructure
4. Weak information infrastructure.

Identification and Assessment of Threats and Opportunities from External Environment

We propose three consecutive steps, which are described in more detail below: 1. Identification of threats and opportunities from external environment; 2. Assessment of threats; 3. Assessment of opportunities. Steps 2 and 3 are described in separate subchapters, thus only basic information is included in this part.

1. Identification of Threats and Opportunities from External Environment

Threats and opportunities from the external environment may be identified in several ways for the analyzed area of the organization. They can be identified through content analysis of initial data followed by some of the creative methods, e.g. brainstorming, consultation, guided discussion aimed at identifying or defining threats and opportunities of the analyzed area of the organization. It is necessary to record the threats and opportunities appropriately e.g. in a form, including the justification of outcomes. A sample form for the identification of threats is shown in Table 3.

Table 3. The sample threat identification form

The analyzed area of organization: *e.g. Security of Organization Information System*	
THREATS	**WHY?** (justification - why we consider a particular factor to be a threat)
A. Monitoring of network	*Weaknesses are detected and data acquired from the information system in order to prepare future attack or compromise the users of information system*
B. Alteration of sent data	*Data are falsified with the aim to introduce disinformation into the information system.*
C. Insertion of disinformation into the information system	*Direct insertion of disinformation (redundant information) into the information system in order to compromise the users of the system.*
D. Overloading of information system	*Make the information system inaccessible by disconnecting it from the communication infrastructure and high-capacity computer networks with the aim to withhold service.*

2. Assessment of Threats

Assessment of threats is primarily aimed at determining the relevance of consequences of threats from the external environment for the analyzed area if they occur. The probability that individual threats occur is discovered. The level of risk that a given threat will affect the analyzed area of organization will then be calculated as a product of threat and relevance of its consequences on an organization and the probability of its occurrence. The higher the level of risk is the bigger strategic significance it has. Then the risks for the analyzed area are arranged according to their levels. The risk of the highest level will be the risk No 1, etc. The way of assessing threats is described in more detail in a special subchapter below.

3. Assessment of Opportunities

It includes determining the attractiveness[2] of opportunity consequence from the external environment on the analyzed area in case it occurs. The probability of occurrence of individual opportunities is determined, too. The benefit of each opportunity may be determined on the basis of the two variables mentioned above. The benefit is determined as a product of attractiveness of opportunity consequence and the probability of its occurrence. The higher the benefit, the bigger strategic significance it has.

Then the benefits for the analyzed area are arranged according to their levels. The benefit of the highest level will be benefit No 1, etc.

The Development of SWOT Matrix

There are two key activities in this phase of developing the SWOT matrix: 1. The recording of factors of strategic significance; 2. The generating of alternative strategies.

1. The Recording of Factors of Strategic Significance

It is the recording of strengths and weaknesses of high relevance as well as the opportunities and threats of high values (i.e. the benefits and risks of high levels), which are of strategic significance. So it is the selection of those factors (strengths, weaknesses, opportunities and threats), which will be used for the generating of alternative strategies.

2. The Generating of Alternative Strategies

The generating of alternative strategies is based on combining strengths and weaknesses (internal factors) with identified threats and opportunities (external factors). The development of four strategies is then a logical continuation of SWOT Matrix (see part b of SWOT Matrix in Figure 2).

SWOT Matrix includes the following four strategies:

- **The WO strategy – the strategy of searching.** These strategies are aimed at overcoming (eliminating) weaknesses by taking advantage of opportunities. These strategies require obtaining additional resources for taking advantage of opportunities.
- **The SO strategy – the strategy of taking advantage.** These strategies take advantage of strengths in favour of opportunities identified in the external environment. This quadrant specifies the desirable condition towards which the organization is heading. It is clear that these strategies are the basis for defining the visions and goals. The difficulty of such a definition and implementation is given by the fact that the S-O combination occurs rarely in real life.
- **The WT strategy – the strategy of avoiding.** It is a defence strategy aimed at the elimination (overcoming) of weaknesses and the avoidance of external threat. It is the “fight for survival” for an organization. If the strategy is used for the development of concepts it is key for maintaining the fundamental functions of the organization necessary for fulfilling its mission.
- **The ST strategy – the strategy of confrontation.** These strategies are possible to be implemented if the organization is strong enough to be confronted with a threat – basically one group of the organization requires that another group of the organization follows the principles of sustainable development.

CASE DESCRIPTION

Attention will be paid to the assessment of the external environment in the following part of the chapter. The first step, the phase of external analysis (the identification and assessment of opportunities and threats), starts with the identification of threats and opportunities (with the help of brainstorming, consultation and guided discussion). Then the threats and opportunities are assessed with the aim to prioritize them according to the relevance and attractiveness of their consequences. The quantified assessment of threats and opportunities may be carried out by number of methods and tools. The assessment of risks and benefits[3] and the matrix of multicriterial assessment may be recommended as the most suitable methodologies.

ASSESSMENT OF THREATS WITH THE USE OF RISK ASSESSMENT

The process of risk assessment[4] may well be used when assessing the already identified threats. The assessed threats represent certain risks, which increase with the relevance of threats. The risks of individual threats results not only from the relevance of their consequences, but also from the probability of their occurrence. Thus the first step of risk assessment is to determine the relevance of the threat from the external environment and its consequences for the analyzed area in case it occurs. The point scale of five basic levels has been set to assess the relevance of threats (see Table 4).

The second step is aimed at describing the probability of a threat occurring. It can be determined in three ways, qualitatively, semi-quantitatively or quantitatively. All three ways of expressing the probability of the threat/opportunity are shown in Table 5.

The quantitative method describes probability mathematically with the help of the following relation (1)

Table 4. The assessment of the relevance of threat consequences

Verbal description of the relevance of threat consequences	**No of points**
Negligible	**1**
Little relevant	**2**
Relevant	**3**
Highly relevant	**4**
Unacceptable	**5**

Table 5. Threat/opportunity occurrence probability assessment

Qualitative expression of probability	Semi-quantitative expression of probability	Quantitative expression of probability [in %]
Almost impossible	**1**	$\langle 1;20 \rangle$
Rarely possible	**2**	$\langle 21;40 \rangle$
Commonly possible	**3**	$\langle 41;60 \rangle$
Highly probable	**4**	$\langle 61;80 \rangle$
Almost certain	**5**	$\langle 81;100 \rangle$

$$P = U \cdot X^{-1} \tag{1}$$

where:
P represents probability that a threat occurs;
U represents the number of undesirable events caused by the assessed threat;
X represents the number of all undesirable events, which happened during the existence of organization.

In case we prefer the semi-quantitative way of expressing the probability of threat it is necessary to compare the final value with Table 5 and to convert the probability expressed in percent into a point scale.

Example: The way of quantitative calculation of probability is exemplified by describing the probability of attack against the organization information system in 2011. The period of existence of the organization is 10 years, in this case from 2001 to 2010. During this time there were 80 serious security attacks against the information system, which is the number of all events during the existence of organization ($X = 80$). The second necessary information is the number of attacks, which were not detected in time and caused undesirable impacts on the organization information system, i.e. the number of completed undesirable events of assessed threat ($U = 23$). After inserting the values into the relation (1) it is calculated the probability of attack against the organization information system in 2011, which is 28.8% ($P = U \cdot X^{-1} = 23 \cdot 80^{-1} = 0{,}288 = 28{,}8\%$). In this case the assumed event is (i.e. the attack against the information system) is rarely probable in 2011 and its value in points is $P = 2$ in the semi quantitative expression of probability (see Table 5).

The following assessment of threats is carried out with the use of risk assessment by inserting the acquired point values into the relation (2)

$$R = C \cdot P \tag{2}$$

where:

R represents the assumed level of risk of a given threat;

C represents the relevance of consequences of the assessed threat;

P represents the probability that the assessed threat occurs.

The final values of individual threats are then compared between each other and used as a basis for the prioritizing of threats. The most relevant threats are considered to be those which have the highest level of risk.

ASSESSMENT OF OPPORTUNITIES WITH THE USE OF BENEFIT EVALUATION

A similar approach may be used in the assessment of opportunities. However, it is necessary first to define the element, which will affect the final order of identified opportunities. Risks defining the most relevant threats for an organization were such elements in case of threats. The assessment of opportunities can be carried out with the use of benefit evaluation, which includes two steps (as in the case of risks). The first step is determining the attractiveness of opportunity consequence from external environment on the analyzed group of processes in case it occurs. The point scale of five basic levels has been set to assess the attractiveness (see Table 6). The second step is aimed at describing the probability that an opportunity occurs. The probability can also be determined in three ways, qualitatively, semi-quantitatively (see Table 5) and quantitatively (see relation 1).

The following assessment of benefits of the analyzed opportunities is carried out by inserting the acquired point values into the relation (3)

$$B = A \cdot P \tag{3}$$

Table 6. The assessment of the attractiveness of opportunity consequences

Verbal description of the attractiveness of opportunity consequences	No of points
Negligible	**1**
Little relevance	**2**
Relevant	**3**
Highly relevant	**4**
Fundamentally relevant	**5**

where:
B represents the assumed benefit of a given opportunity;
A represents the attractiveness of consequences of the assessed opportunity;
P represents the probability that the assessed opportunity occurs.

The final values of individual opportunities are then compared between each other. The opportunities with the highest values are given the highest priority.

ASSESSMENT OF THREATS (OPPORTUNITIES) WITH THE USE OF MULTICRITERIAL MATRIX

The use of multicriterial matrix is another possible and suitable way of assessing the identified threats and opportunities ensuring the objectivity of outcome. In comparison with the previous way of assessment this process can implement, besides the relevance of consequences (or attractiveness) and the level of probability, also other criteria. The criteria will differ depending on the area, which is assessed with SWOT analysis.

The exposure to threat (opportunity) can be considered to be a significant extra criterion. This 'time criterion' introduces another significant factor into the decision-making process, which may fundamentally affect attitude towards the solution of a given area. Another criterion may also be "demand for resources during the development of countermeasures", but its mathematical quantification would probably be demanding and inaccurate, and so its implementation is not recommended.

The first step is based on determining the relevance of consequences (attractiveness) of each threat (opportunity) for a given area, the level of which will be determined with the help of the point scale shown in Table 4 (Table 6 in case of assessing the opportunities). Similarly the probability of each threat (opportunity) will be determined according to Table 5. The exposure (E) will be the last criterion used. It is the ratio of time for which the assessed threat (opportunity) is effective to the time for which the analysis is carried out. This criterion will again be expressed in points from 1 to 5 and its value will be calculated with the help of the following relation (4)

$$E = D \cdot T^{-1} \cdot 100 \tag{4}$$

where:
E represents the final exposure to threat (or opportunity);
D represents the duration of threat (or opportunity);
T represents the time for which the analysis is carried out.

Table 7. The assessment of exposure to threat (opportunity)

Assumed exposure to threat (opportunity) [%]	No of points
⟨1;20⟩	1
⟨21;40⟩	2
⟨41;60⟩	3
⟨61;80⟩	4
⟨81;100⟩	5

The final value expressing the exposure to threat (opportunity) is compared with Table 7 and obtains the corresponding number of points.

Example: Determining the exposure to threat, i.e. the ratio of time for which the threat is effective to the time for which the analysis is carried out, is shown on the following example. The threat "insertion of disinformation into the information system" has been identified within the analysis of external factors of organization. The duration of this threat (D) to the assessed area is estimated to be 3 years, because a new security element protecting the information system against the above mentioned threat is to be installed within 3 years. The time (T) for which the analysis will be carried out is 10 years (i.e. from 2011 to 2020). It can be stated on the basis of the above mentioned that the assumed exposure to this threat is 30% ($E = D \cdot T^{-1} = 3 \cdot 10^{-1} = 0{,}3 = 30\%$) out of the total time during which the analysis is carried out. The value in points will be E = 2.

After determining all criteria, the acquired values are inserted into the prepared Matrix (see Table 9) and the final value of risk (benefit) for individual threats (opportunities) is calculated through arithmetic average (see relation 5). The threats (opportunities) with the highest values are then considered to be the most relevant (attractive).

$$R = C + P + E / 3 \tag{5}$$

where:
R represents the assumed level of risk of a given threat
C represents the relevance of consequence of the assessed threat
P represents the probability that the assessed threat occurs
E represents the exposure to the assessed threat.

Example: The assessment of threats, with the use of multicriterial assessment, is shown in the following case study related to the security assessment of information system in the organization until 2020. The following threats are identified for the above mentioned area within the analysis of external factors:

1. Threat A (T_A): Monitoring of network
2. Threat B (T_B): Alteration of sent data
3. Threat C (T_C): Insertion of disinformation into the information system
4. Threat D (T_D): Overloading of information system.

Three relevant factors were assessed in the analysis of threats: the relevance of consequences (C), the probability of occurrence (P) and exposure (E). The relevance of consequences and the probability of occurrence are assessed in the same way as in the assessment of threats with the use of risk evaluation. The determination of exposure starts from the predetermined fact that the time horizon (T) of analysis is 10 years (from the beginning of 2011 to the end of 2020). This datum is inserted into the relation (4) together with the outcomes of analysis aimed at the duration of threats. Then the exposure to individual threats is calculated. The outcomes are shown in Table 8.

The acquired values of all three criteria are inserted into the multicriterial matrix and the levels of risks (R) of individual threats are calculated (see relation 5) and prioritized from the most to the least relevant. The outcomes are shown in Table 9.

Table 8. The calculation of exposure to the analyzed threats

Threats	*Duration of threat*	*Calculation of exposure*	*No of points*
T_A	*10 years (2011-2020)*	$E = 10 \cdot 10^{-1} \cdot 100 = 100\%$	*5*
T_B	*10 years (2011-2020)*	$E = 10 \cdot 10^{-1} \cdot 100 = 100\%$	*5*
T_C	*3 years (2011-2013)*	$E = 3 \cdot 10^{-1} \cdot 100 = 30\%$	*2*
T_D	*3 years (2011-2013)*	$E = 3 \cdot 10^{-1} \cdot 100 = 30\%$	*2*

Table 9. The example of particular use of multicriterial matrix

MATRIX		**assessment criteria**			*R*	*Order of Threats*
		C	*P*	*E*		
Threats	$\boldsymbol{T_A}$	*2*	*5*	*5*	*4,00*	***1.***
	$\boldsymbol{T_B}$	*4*	*2*	*5*	*3,66*	***2.***
	$\boldsymbol{T_C}$	*3*	*1*	*2*	*2,00*	***4.***
	$\boldsymbol{T_D}$	*4*	*1*	*2*	*2,33*	***3.***

MULTICRITERIAL ASSESSMENT OF THREATS (OPPORTUNITIES) WITH REGARD TO THE SCALES OF CRITERIA

The previous use of multicriterial assessment assumes that all the applied criteria are equal, i.e. they have the same coefficient of relevance. However, it will be necessary to take the scales of individual criteria into account if we want to achieve a more accurate outcome. It is a numerical expression of their relevance, or, the accuracy of estimate, or predictability. The general rule[5] will be applied that the more relevant the criterion is (or, more precisely, the more relevant it is considered to be by a decision maker) the higher its scale is. Lower scales, on the contrary, will be assigned to less relevant criteria.

The scales of criteria may be determined by various methods, e.g. by pair comparison, 100 points method, and Saaty´s method. However, in case there is a small number of the assessed criteria (3 criteria in our case, i.e. the relevance or attractiveness of consequences, the probability of occurrence and exposure) it is reasonable to use the method of direct determining of criteria scales with the help of the point scale. The point scale of lower discrimination ability from 1 to 5 has been used for determining the scales, where 5 points are the most significant, while 1 point is of little significance. The outcome of assessing the relevance of criteria based on the graders´ preferences is shown in Table 10.

After determining the scales of criteria it is possible to continue with the multicriterial assessment. The procedure will be similar as in the previous case, i.e. the acquired values of all criteria will again be inserted into the Matrix and the final levels of risks (benefits) will be calculated for individual threats (opportunities). The calculation is different from the previous one in considering the determined criteria scales, which multiply individual criteria. The final value of risk (opportunity) will be calculated as a sum of weighted values of individual criteria (see relation 6). The threats (opportunities) of the highest values are considered to be the most relevant (attractive).

$$R = C \cdot S_C + P \cdot S_P + E \cdot S_E \qquad (6)$$

Table 10. The determining of criteria scales with the help of point scale

Criterion	C (A)	P	E	Sum
No of points	5	5	3	13
Standard scales	**0,385**	**0,385**	**0,230**	1

where:
R represents the assumed level of risk of a given threat
C represents the relevance of consequences of the assessed threat
P represents probability that the assessed threat occurs
E represents exposure to the assessed threat
S represents standard scales for individual criteria.

Example: We will continue with the previous example to demonstrate the multicriterial assessment of threats with regard to the criteria scales. At first the standard scales (see Table 10) are added to the acquired values of criteria (C, P, E) and thus the criteria will achieve different relevance. After that all data are inserted into the multicriterial matrix and the risks for individual threats are calculated. The final step is aimed at prioritizing the threats according to the final values of risks, i.e. the threats of the highest values are the most relevant (see Table 11).

After the multicriterial assessment is finished and the threats are prioritized according to the levels of risks the threats are recorded in an appropriate form, similarly as in the case of strengths and weaknesses. After that the threats are prioritized according to the achieved levels of risks (from No 1 for the threat of the highest level of risk to No X for the threat of the lowest level of risk). The threats in our case study are prioritized according to their levels of risks as follows:

1. Monitoring of network
2. Alteration of sent data
3. Overloading of information system
4. Insertion of disinformation into the information system.

Table 11. The example of multicriterial matrix used with regard to criteria scales

MATRIX		**assessment criteria**			*R*	*Order of Threats*
		C	*P*	*E*		
THREATS	T_A	*2 · 0,385 = 0,77*	*5 · 0,385 = 1,925*	*5 · 0,23 = 1,15*	*3,85*	***1.***
	T_B	*4 · 0,385 = 1,54*	*2 · 0,385 = 0,77*	*5 · 0,23 = 1,15*	*3,46*	***2.***
	T_C	*3 · 0,385 = 1,155*	*1 · 0,385 = 0,385*	*2 · 0,23 = 0,46*	*2,00*	***4.***
	T_D	*4 · 0,385 = 1,54*	*1 · 0,385 = 0,385*	*2 · 0,23 = 0,46*	*2,39*	***3.***

SOLUTIONS AND RECOMMENDATIONS

Every analyst must ensure that the outcomes of assessment are the most objective. This is true also in case of assessing the security of organization security systems through SWOT analysis. The level of subjectivity in the analytical process is minimized by implementing the above presented methods, which increases the quality of the acquired information. Objective outcomes help the organization to have a more precise overview of the prospects of further development.

The assessment of risks and benefits is a suitable way of acquiring the objective outcomes in the assessment of external factors. It is based on the assessment of two basic criteria, the relevance or attractiveness of consequences and the probability of their occurrence. The matrix of multicriterial assessment may also be used for the assessment of threats and benefits. The advantage of this type of assessment is in implementing more criteria, the predictability of which may be considered through standard scales. On the other hand there are also some disadvantages – it is time consuming, and criteria may be selected and assessed inappropriately. At the same time it has to be stated that theoretical knowledge and, ideally, experience are the necessary prerequisites for the implementation of these methods.

The implementation of SWOT analysis is fundamentally based on specific methods and tools, which are implemented in the identification of external and internal factors as well as in their assessment. Therefore it is suitable to analyze the possibilities of implementing the methods and tools for specific types of organizations in individual phases of SWOT analysis. The future research should be aimed at discovering the possibilities of other suitable semi quantitative and quantitative methods of assessing the strengths, weaknesses, opportunities and threats. The research aimed at discovering the purpose of implementing SWOT analysis in individual organizations of the private and public sector could also provide interesting information.

ACKNOWLEDGMENT

Language correction was done by Jiří Dvořák from University of Defence, Czech Republic. This chapter has been developed within the project of the Ministry of Interior of the Czech Republic, filed under VF20112013019code and entitled ‘Objectification of Threats and Risks of Equipments for the Production and Transmission of Electricity’.

REFERENCES

Fotr, J. (2006). *Managerial decision making*. Prague, Czech Republic: Ekopress.

Grasseova, M. (2006). The implementation of SWOT analysis in long-term planning. *Defence and Strategy, 2*(6), 48-55. ISSN 1214-6463

Grasseova, M., Dubec, R., & Horak, R. (2008). *Procedural management in public and private sectors*. Brno, Czech Republic: Computer Press.

Grasseova, M., Dubec, R., & Rehak, D. (2010). *The analysis of enterprise on manager's hands: 33 the most frequently applied methods of strategic management*. Brno, Czech Republic: Computer Press.

Rehak, D., Dubec, R., & Grasseova, M. (2008). *Assessment of external environmental elements within SWOT analysis utilizing the evaluation of risks and benefits.* Paper presented at the Symposium on Risk Analysis /Management Cybernetics /Economics (19th International Conference on Systems Research Informatics & Cybernetics), Baden-Baden, Germany.

Rehak, D., & Dvorak, J. (2010). Risk catalogue as a software tool for supporting the business continuity planning. *Int. J. Business Continuity and Risk Management, 1*(2), 187-196. ISSN 1758-2164

Rehak, D., Dvorak, J., & Grasseova, M. (2009). Principles, framework and process of risk management. In J. Navrátil & J. Barta (Ed.), *International Conference Security Management and Society* (pp. 364-376). Brno, Czech Republic: University of Defence. ISBN 978-80-7231-653-3

Tomecek, P. (2008). The methods of computer attacks in the information warfare. In P. Hruza & P. Tomecek (Ed.), *The 2nd International Conference on Advanced and Systematic Research.* (pp. 79-82). Zagreb, Croatia: Faculty of Teacher Education of the University of Zagreb. ISBN 978-953-7210-14-4

KEY TERMS AND DEFINITIONS

Assessment of Risks and Benefits: The assessment of risks (benefits) is carried out by determining the relevance (attractiveness) of consequences of the analyzed threats (opportunities) in the assessed area of organization and defining the probability of threats affecting the given area.

Attractiveness of Consequences: The attractiveness of opportunity consequence is the value derived from the amount of potential benefits caused for the organization by taking advantage of such an opportunity.

Multicriterial Assessment: The multicriterial assessment is based on the assessment of factors of the analyzed area (e.g. threats and opportunities) with the help of predetermined criteria (e.g. the relevance of consequences, the probability of occurrence or exposure).

Opportunities: Factors from the external environment of organization, which may be used by an organization to increase its effectiveness and efficiency.

Probability: Probability is the value, which expresses the degree of predictability that a threat or an opportunity will affect the assessed area of the organization.

Relevance of Consequences: The relevance of consequences is the value derived from the amount of potential losses caused for the organization by threats.

Strengths: The internal factors of organization, which have positive effect on its effectiveness and efficiency.

SWOT Analysis: SWOT analysis is a method of strategic analysis of the initial state of organization and/or its part generating the alternatives of strategies on the basis of internal analysis (strengths and weaknesses) and external analysis (opportunities and threats).

Threats: Factors from the external environment of organization, which may threaten the effectiveness and efficiency of the organization.

Weaknesses: The internal factors of organization, which have negative effect on its effectiveness and efficiency.

ENDNOTES

1. Grasseova et al. (2010, pp. 304).
2. The term attractiveness of opportunity consequence shows the extent to which the given opportunity is beneficial and applicable for the analyzed group of processes.
3. Rehak et al. (2008).
4. Rehak et al. (2009), Grasseova et al. (2010) and Rehak and Dvorak (2010).
5. Fotr (2006) and Grasseova et al. (2010).