Defining a cybersecurity strategy of an organization: criteria, objectives and functions

I.V. Mandritsa
North-Caucasus Federal University, Russia
d_artman@mail.ru
V.I. Peleshenko
North-Caucasus Federal University, Russia
viper@26.ru
O.V. Mandritsa
Russian Technological University - MIREA Stavropol branch office, Russia
man_olga@mail.ru
A. Fensel
University of Innsbruck, Austria
anna.fensel@uibk.ac.at
F.B. Tebueva
North-Caucasus Federal University, Russia
fariza.teb@mail.ru
V.I. Petrenko
North-Caucasus Federal University, Russia
vipetr@mail.ru
I.V. Solovieva
North-Caucasus Federal University, Russia
solovyeva_ira@mail.ru
M. Mecella
Sapienza Università di Roma, Italy
massimo.mecella@uniroma1.it

Abstract

The paper addresses strategic planning of the cybersecurity of an organization. A mathematical model for setting the strategic plan is proposed.

Keywords: strategic planning of cybersecurity; criteria and objectives of the mathematical model; factors of the model

1 Introduction

European countries have adopted a common cybersecurity strategy of the states (for both the public, including military, and private sectors). It proposes that the development of cybersecurity capabilities "focus on the detection, response and recovery from complex cyber threats" that have taken place [1]. The strategy is based on synergy "between civil and military approaches to the protection of critical cyber assets". The basis for the development of the strategy was to take a qualitative methodological approach consisting of: data collection, desk study questionnaires and a series of consultations and interviews with experts, covering 17-member States of the EU, stakeholders from the public and private sectors. The validation of the findings was carried out in a workshop organized in the Hague in cooperation with ENISA and the NCSS ENISA expert group in 2017 [2].

For USA, the main goal of strategy for 2023 is that "the Department of Homeland Security (further DHC) will have improved national cybersecurity risk management by increasing security and resilience across government networks and critical infrastructure; decreasing illicit cyber activity; improving responses to cyber incidents; and fostering a more secure and reliable cyber ecosystem through a unified departmental approach, strong leadership, and close partnership with other federal and nonfederal entities" [3]. That is why the second guiding principle of

In: Marco Schaerf, Massimo Mecella, Drozdova Viktoria Igorevna, Kalmykov Igor Anatolievich (eds.): Proceedings of REMS 2018 – Russian Federation & Europe Multidisciplinary Symposium on Computer Science and ICT, Stavropol – Dombay, Russia, 15–20 October 2018, published at http://ceur-ws.org

cybersecurity strategy is based on "cost-effectiveness. Cyberspace is highly complex and DHC efforts to increase cybersecurity must be continuously evaluated and reprioritized to ensure the best results for investments made".

The aims of cybersecurity strategy in Canada are formulated similarly. Cybersecurity is a shared responsibility, and requires close partnership between the federal Government, the private sector, other levels of government, international partners, and Canadians to ensure that vital cyber systems are secure, and that Canadians can go online with confidence. The Strategy and the Action Plan reflect this shared responsibility [4].

Considering the strategic plan of the cybersecurity of the organization (further CSO) like a system of case-operations of an information system (further IS) which aims to condition managing of its cyber protection, it has been noted that each of the carried-out activities of an administration, is an expensive process (spending on, cost of IS). As the resources and budgets of the organizations are limited, the issue of choosing the rational composition of case-actions to improve the organization's cyber-security is the main objective of the strategy.

2 Discussion

We share the view [5], that regular strategic management can be represented as a process that determines the sequence of actions of the organization for developing and implementing a strategy (in our context - the strategy of cybersecurity and its main indicator of the cyber-protection). Cybersecurity is the process of developing methods, security policies and implementing measures to protect information systems, networks, and cyberspace applications of the organization from digital (computer) attacks. In itself, the process of strategic planning involves setting goals for achieving the future state of high cybersecurity of the organization, and, accordingly, developing the strategy that will enhance it, by identifying the necessary resources and methods of protection by developing case studies on the channels of organization threats.

Further, the strategic management of cybersecurity has emerged through evolutionary development from the strategic planning of the state of cybersecurity of the information environment of the organization, which constitutes its essential basis. The essence of the changes, which have taken place in the information environment of the organization from the position of cybersecurity, is reduced to breaking up the process of strategic planning of its cybersecurity into three interrelated, but at the same time independent, activities corresponding to the basic functions of cybersecurity management: *(1)* development of the cybersecurity strategy based on an analysis of the external and internal environment of the information environment of the organization, consideration of possible alternatives; *(2)* organization of the strategy (case-based cybersecurity) by the criterion of maximum cybersecurity with a minimum of cost options; *(3)* monitoring and evaluation of the results of cybersecurity, before and after implementation of case-events.

We will also consider the issue of forming an economically effective (rational) strategic plan for the CSO. We will determine that the efficiency of the strategic plan of the CSO is understood as the maximum of the ratio of the final level of the cybersecurity of the organization, in the form of the ratio of the amount of value available to the organization, methods of countering threats (the cost of the reporting period for the activities) to its initial (basic) level. From a mathematical point of view, it can be seen that all the factors affecting the input Y_{ij} or the output parameters of CSO object X_i, causes changes in its state of cybersecurity from the position of its effectiveness. Hence, for describing the model of strategic management of cybersecurity of the organization, that along with the cost process (IS case-events), it is necessary to consider input and output values of the probability of threats for the whole system of CSO, and also any external factors affecting them. There are many parameters for accounting of the CSO mathematical model.

3 The model

The formalization of cybersecurity has as a cumulative state of cybersecurity of some organization X_{cs}, which has three components in its composition:

$$X_{cs} = \sum SI_X + SNet_X + SInet_X \tag{1}$$

where SI_X – information security of an object , $SNet_X$ – network security of an object , $SInet_X$ – Internet security of an object .

Accordingly, the target function of the cybersecurity economy of the object X, in the form of cybersecurity index of the information environment of this organization X, will tend to expression:

$$f(X) \to maxBcS \tag{2}$$

However, cybercrime can be seldom estimated with a certain probability e.g. that the threat of cyber information leakage will appear or not appear for the object X. From the position of the economics, it has two characteristics: the probability of occurrence and the amount of possible future damage from loss of cyber information. The formula of risk of threats of leakage and possible damage for cyber information R (RE) is:

$$R = \rho U(Threat) * CU(Threat) \tag{3}$$

where: $\rho U(Threat)$ – the likelihood of a threat of damage to cyber information, as a relative number; $U(Threat)$ – the amount of possible damage from the leak (loss) of cyber information, as a monetary value.

Introducing the categories of risk and the severity of threats from the leak, "Damage of loss" of cyberinformation (leaks) should be introduced. Accordingly, equation (1) is converted to the following one:

$$X_{cs} = \sum SI_X + SNet_X + SInet_X - \rho U(Threat) * CU(Threat)(X_{cs}) \tag{4}$$

The parameters of the initial CSO system will be considered as parameters of the model. We will define the list of them in the form of the X_{CSO} vector:

$$X = \{X_j, j = 1 \dots n\} \tag{5}$$

In our case, x_1, x_2, $\dots x_n$ is a list of possible strategic, costly planned case-events of the IS. In this case, n is the number of blocks of the lowest level of the strategic plan. There are some limitations on the interrelated parameters of the system of strategic case-events. The functioning of the CSO system is determined by a set of target characteristics which depend on the parameters of this system :

$$F(X) = \{f_k(X), k = 1..K\} \tag{6}$$

In the case of strategic planning of the CSO $K_{IS} = 3$.

The objective characteristics of the strategic cost-intensive business events of IS are:

1. The effectiveness of investing in the protection of information security, the level of risk for each channel of threats, the degree of strategic significance of this IC activity as part of the strategic plan of the CSO. We denote them by $f1$, $f2$ and $f3$, respectively.

2. The effectiveness of investing in the protection of information security in this case will be considered as the profitability of a separate strategic activity of the IS for assessing the cybersecurity of the CSO. The mathematical formulation of the multicriteria task of ranking the operational case-events of information security for the process of enhancing the cybersecurity of the organization X is presented in Figure 1. Let us dwell in more detail on the determination of the level of risk through the channels of threats of the CSO. We propose the following methodology for assessing the level of risk:

   - Identifying the full set of risks of a strategic case study for protecting IS of the organization Figure 1.
   - Expert poll and determination of the strategic goal-setting levels affecting this i-th risk of the case-study of the strategic plan of the CSO, $i = 1 \dots I$.
   - Determination of the dimension (area) of the matrix of the cumulative risk of the strategic case-event IS: since the number of levels of strategic goal setting is seven, then $7 * I$.
   - Determination of the risk field area S_{risk} as the number of risk units of the matrix of the combined risk of the strategic IS case-study.
   - The level of risk can be determined by the formula: $f_2 = \frac{S_{risk}}{7*I}$

3. The degree of strategic importance of the IS event is proposed to be determined expertly as the degree of influence given to the event-action on the final result of the strategic plan of the IS (in fractions of a unit).

The degree of strategic importance of the IS activity can be determined as the degree of influence of this IC activity on the final result of the strategic plan (in fractions of a unit). The optimization problem here comprises choosing from the set of acceptable values such parameters of cyber-security of the whole IS organization, so that its performance indicators (target characteristics of cybersecurity through threat channels) are in the optimal range. For our case, the indicators should be maximal: $f_k(X) \to max, k = 1 \dots k$

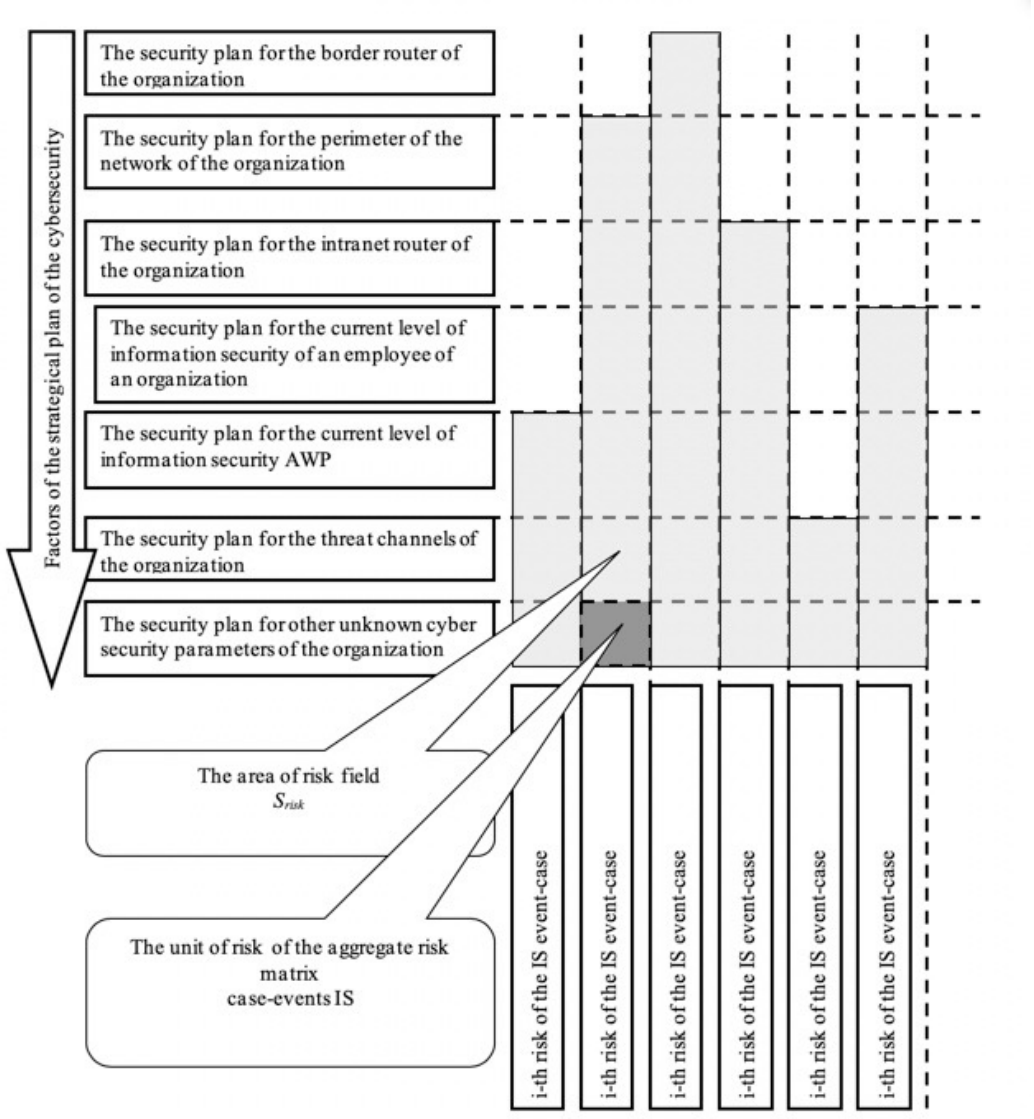

Figure 1: Factors for assessing the level of risk for the adoption of a strategic plan of the organization

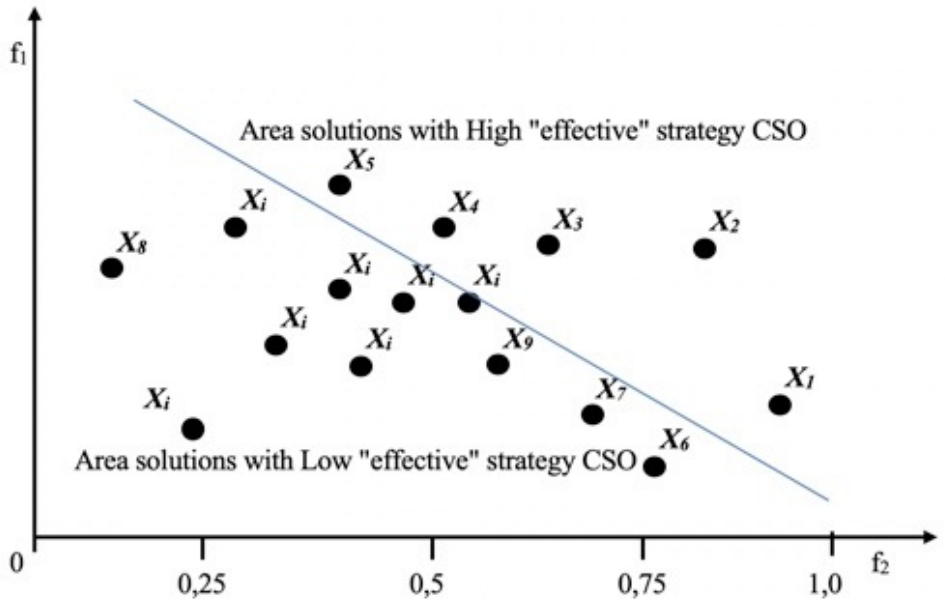

Figure 2: Correlation of Pareto sets in coordinates effectiveness of investment in case-activities IS - level of risk of CSO

Assuming the non-negativity condition x_i as a constraint, we obtain a system of equations and restrictions: $x_i > 0$. If the values of the optimum X_i* obtained by solving the problem for each criterion do not coincide, then the solution of the problem can be only a compromise solution that satisfies all the components of the vector criterion $F(X)$. A point $X0$ satisfying the conditions below is Pareto optimal if there is no other point $X1$ for which $f_k(X1) > f_k(X0)$.

And the strict inequality should be completed at least for one of the criteria. A set of such points is called a Pareto set. They are also called the set of "unimprovable points", because you cannot find such other point for any of them, so that one of the criteria improves, and the rest do not deteriorate. For each case-event, depending on the value of the indicators of the amount of investment, risk level, the degree of strategic importance of the IS activities in the composition, the strategic plan of the CSO will assign an appropriate rank, and the maximum rank will correspond to the IS event, the investment of which should be primarily implemented. We represent the solution with a point on the plane with the coordinates $f1$ and $f2$. We number the points according to the number of the solution (cf. Figure 2).

Following the indexes of the Figure 2, only the solutions $x1$, $x2$, $x3$, $x4$, $x5$ lying on the right upper boundary of the domain of possible solutions for the protection of information security as part of the overall strategic plan of the CSO are optimal. For any other solution of the IS $_i$, there is at least one dominant, for which both $f1$ and $f2$ are greater than for x_i. The allocated "effective" set of solutions for protecting the IS will be the Pareto set. This set will be "effective" according to two criteria - minimum costs for a case-event and maximum security. By applying the criterion $f3$ to the IS events of this set, we will receive a list of IS case-events for implementation in order of decreasing of their strategic importance of the all cybersecurity.

Thus, we get a many solutions to the index of cyber-security of the CSO, which will be less effective than the first one. If we continue this process, we can obtain a sequence of solutions sets - successive Pareto sets, where each set will be less efficient than the previous one, but more effectively than the subsequent one. Within a specific set, the priority of decisions in descending order of their strategic importance is determined by the ranking of the case-activities of the IS of the given set by the criterion $f3$.

The lesser number of successively less "effective" sets of strategic costly business events, that IS can achieve the main goal of the strategy (the maximum cybersecurity of the organization), the higher its effectiveness is. Obviously, this process should be iterative with correction of business processes of the strategic plan. Another theory of multi-criteria sets is one of the approaches to solving multicriteria problems that most adequately

reflect the conditions of functioning of the systems under consideration.

The theory of fuzzy sets allows best to structure everything that is divided by not very clear boundaries. To this end, membership functions that characterize the degree of closeness of a given element to a given set are considered in the theory of fuzzy sets. Let's consider the solution of the problem posed by the theory of fuzzy sets.

Let $X = \{x_1, x_2, x_3, \ldots, x_n\}$ be the collection of some objects. Then the fuzzy set L is the set of ordered pairs:

$$L = \{(x, \mu_l(x_i)), x_i \in X\} \tag{7}$$

where $\mu_l(x_i)$ is the degree of belonging of x_i to L. The function μ_l is called the membership function.

In our case, we assume that $\mu_l(x_i) \in [0 \ldots 1]$. Thus, the fuzzy set L, despite the indistinctness of its boundaries, can be determined by comparing to each object x_i a number lying between 0 and 1. Two fuzzy sets L and M are said to be equal if and only if $\mu_l(x_i) = \mu_m(x_i)$, for all $x_i \in X$. The intersection of fuzzy sets L and M is a fuzzy set, denoted by $L \cap M$ and it has the following membership function:

$$\mu_{L \cap M}(x_i) = min(\mu_l(x_i), \mu_m(x_i)), \forall x_i \in X \tag{8}$$

A fuzzy goal $f(X)$ will be identified with a fixed fuzzy set L in X, and a fuzzy restriction $g(X)$ with a fuzzy set. Then the fuzzy set F formed by the intersection of L and M is called the effective solution of the CSO's cybersecurity, i.e. $F = L \cap M$.

The main drawback of this method is the subjectivity of the administrative expert, who decides on the choice of a particular function.

Next, we suggest using a well-known technique of constructing the membership function, based on the ranking of the original arrays. We arrange the IS activities in order of increase in one of the given parameters - in order of increasing of profitability of investing in the protection of information security. Then, for each IS event, we determine the value of n/N, where n is the serial number of the strategic case-event of the IS in an ordered sequence, and N is the total number of strategic costly case activities.

Next, graphs are plotted in a coordinate system with the axes "Cyber-security - n/N", "Risk level - n/N"and "degree of strategic significance - n/N"and approximate the resulting point dependences. As a result, we get three functional dependencies:

$\boldsymbol{\mu_1 = \mu(f_1)}$ (cybersecurity),
$\boldsymbol{\mu_2 = \mu(f_2)}$ (level of risk),
$\boldsymbol{\mu_3 = \mu(f_3)}$ (degree of strategic importance)

which we will consider as a membership function. The use of these functions essentially means the normalization of the initial criteria. Next, we can use the verification of the criteria for obtaining the principle of optimality. As a verification, we consider the function:

$$\boldsymbol{\mu = \sqrt[n]{\mu_1 \mu_2 \mu_3}} \tag{9}$$

Each cost-based case-event of the IS corresponds to a specific parameter value μ. The maximum value of the parameter μ corresponds to the strategic expenditure event IS, in which prevention it must be invested in the first place. Minimum - a costly IS event, which prevention can be implemented in the last turn. Thus, when reducing threats for object X, we will reach the maximum-reasonable limit of cybersecurity of the object. As a result, the overall value of the current protection of the subject's cyber security can be expressed by the following indicator - the coefficient of cyber security protection K_{CSP}[6] which will be based on the ratio of economic indicators:

$$K_{CSP}(X) = \frac{\sum Z_{protectionofcyberinformation}(X_{CS})}{S_{costofcyberinformation}(X_{CS})} \tag{10}$$

where $\sum Z$ is protection of cyber information (X) is an mount of funds for the protection of cybersecurity throughout the facility and its component components for X_{CS};S is the cost of funds for the creation of cyber information on the zones of cybersecurity of the object X_{CS}.

4 Concluding remarks

This assessment, along with other procedures, can be reflected in the methodological approach to transformations. The essence of the process of increasing the cybersecurity of the CSO allows to choose two directions for evaluating its results.

The first direction requires the efficiency index of increasing the cybersecurity of the CSO as the ratio of all the components of the effect from the conducted case-events to all costs associated with the implementation of the cybersecurity transformation process.

The second direction considers the informational adaptation of an organization, which manifests itself in improving, reaching a new level of the response speed of an organization to the effects of external threats as the main result of increasing the cybersecurity of the CSO. For example, the components of the effect for the whole organization can be achieved through:

- implementation of IS case-events at the level of software used on all channels of the organization;
- streamlining the IS case-events for informational flows and the composition of informational arrays, including input, intra-system and output information of the whole organization;
- implementation of IS case-events for each employee of the organization;
- implementation of the IS case-events at the hardware level as a result of the strategic plan of the : conservation, access control, write-off of unused and worn out workstations.

The main components of the cost of interventions of IS case-events for the organization are:

- the costs of improving the IS protection in terms of the organizational units of an organization in terms of implementing the strategic planning system;
- attracting expert advisors for information and economic security;
- training and retraining of the personnel in the IS part;
- maintenance of the management of the organization.

The merits of the model include the fact that it allows to determine the actual amount of the effect of the cyber-protection of an organization on the money invested in the implementation of the strategic plan of the . At the same time, the changes in the effectiveness of the cybersecurity of an organization as a whole as a result of the process of increasing the cybersecurity of the are not reflected in this work.

References

[1] *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* Brussels, 7.2.2013, JOIN (2013) 1 final.

[2] European Union Agency for Network and Information Security (ENISA). *Information sharing and analysis centres (ISACs).* ISBN: 978-92-9204-239-4, DOI: 10.2824/549292

[3] U.S. Department of homeland security. *Cybersecurity strategy.* May 15, 2018

[4] Government of Canada. *Action Plan 2010-2015 for Canada's Cyber Security Strategy.* ISBN: 978-1-100-21895-3.

[5] King, W.R. and Cleland, D.I. *Strategic Planning and Policy*, New York: Van Nostrand-Reinhold , 1978.

[6] Boehm, B.W. Software Risk Management: Principles and Practices. *IEEE Software*, Volume 8, Number 1, January 1991, pp. 32-41

[7] Mandritsa I.V., Mandritsa O.V., Solovieva I.V., Petrenko V.I. Method of justification of expenses on information security of the budgetary organizations. *Bulletin of the North Caucasian Federal University*, 2017, no. 1 (58), pp. 67-71.