Choosing the optimal strategy for information security in a business organization

A. CHOJNACKI, G. PIENIĄŻEK
andrzej.chojnacki@wat.edu.pl, grzegorz.pieniazek@gmail

Military University of Technology, Faculty of Cybernetics
Kaliskiego Str. 2, 00-908 Warsaw, Poland

The paper describes the method of choosing the optimal strategy to implement security measures in a business organization. Strategies are categorized depending on time horizons, the history of threats and implemented security measures. Next, the method of choosing the optimal strategy for a business organization in a given context is outlined. Then this method is used to select the optimal strategy in a particular business context. The method is based on a deterministic time-based information security model, which was extended to a random model. With this simulation method, an organization can choose a strategy to implement security measures that best suits its needs. It is important for organizations to conduct an analysis of costs and threats in order to select appropriate safeguards.

Keywords: information security, stochastic model, simulation.

1. Introduction

There are *P* business processes implemented in a business organization [12]. We analyze the actions of a business organization in *T* time periods during which a *V* number of threat types may occur [8]. Let the intensity of the occurrence of a v type of a threat in the time period t be $X_v(t)$.

The history of the occurrence of threats to the time period t, with this time period included, will be denoted by

$\mathcal{X}(t) \triangleq \langle \mathbb{X}(t), \mathbb{X}(t-1), \mathbb{X}(t-2), ..., \mathbb{X}(1) \rangle$,

where $\mathbb{X}(t) \triangleq [X_1(t), X_2(t), ..., X_V(t)]$.

If there appears no threat, the financial effect on the completion of the business process p in the time period t will be $L_p(t)$.

In order to counteract the adverse effects of the occurrence of threats, an organization can implement an I number of types of safeguards [8]. Let $s_i(t) \in \{0,1\}$ mean the decision to initiate the implementation of solution i in the time period t, if $s_i(t) = 1$, and the lack of such a decision if $s_i(t) = 0$. The history of the use of safeguards by the organization can be described as follows:

$$\mathbb{S} \triangleq \begin{bmatrix} s_1(1) & ... & s_I(1) \\ ... & ... & ... \\ s_1(T) & ... & s_I(T) \end{bmatrix}_{TxI}$$

After the decision to implement the i type safeguard in the time period t, it is implemented within $G_i(t)$ time units. Then it works with $\overline{O}_i$ intensity for $r_i(t)$ time units and then it ceases to function. The organization allocates a $\overline{\Gamma}(t)$ sum of money for the implementation and maintenance of all safeguards in the time period t [8].

The cost of the implementation and functioning of the i type safeguard in time period t is related to the business process p If in the time period n a decision was made to implement this safeguard, it is denoted by $e_i^p(n,t)$.

Moreover, the occurrence of threats to the time period t described as $\mathcal{X}(t)$, using safeguards in accordance with the decisions described in the $\mathbb{S}$ matrix, reduces the financial effects of the business processes, which for the process p are denoted by $\Phi_p(\mathcal{X}(t), \mathbb{S})$.

The above quantities describing the functioning of a business organization at a hazard of information threats are presented in [5], with additional properties outlined in detail.

The model is deterministic in nature, i.e. the threats described by the $\mathbb{X}(T)$ matrix are considered as known a priori. In fact, the information on the risk of a threat is obtained on an ongoing basis, after the occurrence of threats. This entails that during the development of a safeguard management strategy we have to rely on incomplete information. In practical terms, statistical data on the prevalence of threats are often available to the general public. In this paper we treat $X_v(t)$ quantities as random variables with known discrete distribution, and we assume that these random variables are stationary and pairwise independent, assuming the values from the $\overline{\mathbb{X}}_v$ sets. Realization of a random variable $X_v(t)$ is denoted by $\overline{X_v}(t)$. The vector of a realization of a random variable $X_v(t)$ in time period t is denoted by $\overline{\mathbb{X}}(t) \triangleq \left[\overline{X_1}(t), \overline{X_2}(t), ..., \overline{X_V}(t)\right]$.

2. Safeguard Implementation Strategy

Let c mean the number of time periods for which the organization stores data about $\overline{X_v}(t)$ values. The organization may have data for the ranges with numbers smaller than one, for business activity conducted before the one analyzed in the model. Moreover, let h mean the number of time periods for which the organization has data on the distribution of random variables $X_v(t)$. Both c and h values may depend on the time and the possible types of threats.

When making decisions about the implementation of safeguards in subsequent time periods, a business organization analyzes its state, the history of threats and random variables describing future threats. At this point it is worth reminding that the description of the organization's state comprises:

- information about the time when each of the safeguards ceases to function,
- information about when each of the safeguards becomes operational,
- limit of money to be spent on security measures.

Safeguard implementation function is expressed as follows:

$$\begin{aligned}&\mathrm{Z}\Big(t, y, \overline{\mathbb{X}}(-c), \overline{\mathbb{X}}(-c+1), ...\\ &..., \overline{\mathbb{X}}(t), \mathbb{X}(t+1), ..., \mathbb{X}(T+h)\Big) = s(t)\end{aligned} \qquad (1)$$

which means making the decision $s(t) = \left\langle s_1(t), ...s_I(t)\right\rangle$ in state *y*, in time period *t*, with a known history of the occurrence of threats denoted by $\overline{\mathbb{X}}(t-c), \overline{\mathbb{X}}(t-c+1), ..., \overline{\mathbb{X}}(t)$, and with information about the distribution of random variables denoted by $\mathbb{X}(t+1), ..., \mathbb{X}(t+h)$.

A sample classification of safeguard implementation strategies is outlined below. The first group comprises strategies independent of threat history and, at the same time, independent of the anticipated threats.
The strategies in this group are reduced to:

$$\mathrm{Z}(t, y) = s(t) \qquad (2)$$

Sample strategies for this group include:

- no implementation of any kind,
- implementation of the most expensive safeguards only,
- implementation of the biggest number of safeguards,
- implementation of randomly chosen strategies with a fixed probability distribution.

Strategies dependent on threat history but independent of anticipated threats constitute the second group. These strategies may take into account threat history for $c^{'}(t) \leq c$ proceeding time periods at a fixed and variable horizon. Strategies belonging to this group can be represented as, for example:

$$\begin{aligned}&\mathrm{Z}\Big(t, y, \overline{\mathbb{X}}\big(t-c'(t)\big), \overline{\mathbb{X}}\big(t-c'(t)+1\big), ...\\ &..., \overline{\mathbb{X}}(t)\Big) = s(t)\end{aligned} \qquad (3)$$

or

$$\mathrm{Z}\Big(t, y, \overline{\mathbb{X}}(-c), \overline{\mathbb{X}}(-c+1), ..., \overline{\mathbb{X}}(t)\Big) = s(t) \quad (4)$$

In the second case, all available history is taken into account in the decision-making process. Examples of strategies belonging to this group include:

- counteract threats that occur most frequently,
- counteract threats that bring the biggest losses,
- counteract threats that have not occurred so far,
- counteract threats that have occurred recently.

The third group are strategies independent of threat history but dependent on anticipated threats. These strategies can use threat anticipation for $h^{'}(t) \leq h$ time periods ahead at a fixed and variable horizon. Strategies belonging to this group can be represented as, for example:

$$\mathrm{Z}\left(t, y, \mathbb{X}(t+1), ..., \mathbb{X}(T+h)\right) = s(t) \tag{5}$$

or

$$\mathrm{Z}\left(t, y, \mathbb{X}(t+1), ..., \mathbb{X}\left(t+h'(t)\right)\right) = s(t) \tag{6}$$

For the first function, the anticipation horizon is fixed.

Examples of strategies belonging to this group include:

- stay ahead of the most likely threats,
- stay ahead of threats that cause the most expensive losses
- stay ahead of threats with the greatest risk of occurrence [8], [11], [12].

The fourth group comprising strategies dependent on threat history and at the same time on the anticipated threats, is the most general group of strategies. These strategies may take into account threat history for $c^{'}(t) \le c$ preceding time periods at a fixed and variable horizon. They can use threat anticipation for $h^{'}(t) \le h$ time periods ahead at a fixed and variable horizon. Strategies belonging to this group can be represented as in (1) or as one of the following variants:

$$\begin{aligned} &\mathrm{Z}\Big(t, y, \overline{\mathbb{X}}\left(t-c'(t)\right), \overline{\mathbb{X}}\left(t-c'(t)+1\right), \ldots \\ &..., \overline{\mathbb{X}}(t), \mathbb{X}(t+1), ..., \mathbb{X}(T+h)\Big) = s(t) \end{aligned} \tag{7}$$

or

$$\begin{aligned} &\mathrm{Z}\Big(t, y, \overline{\mathbb{X}}\left(t-c'(t)\right), \overline{\mathbb{X}}\left(t-c'(t)+1\right), ... \\ &\ldots, \overline{\mathbb{X}}(t), \mathbb{X}(t+1), ..., \mathbb{X}\left(t+h'(t)\right)\Big) = s(t) \end{aligned} \tag{8}$$

or

$$\begin{aligned} &\mathrm{Z}\Big(t, y, \overline{\mathbb{X}}(-c), \overline{\mathbb{X}}(-c+1), ... \\ &\ldots, \overline{\mathbb{X}}(t), \mathbb{X}(t+1), ..., \mathbb{X}\left(t+h'(t)\right)\Big) = s(t) \end{aligned} \tag{9}$$

Sample strategies belonging to this group involve being ahead of:

- the most likely threats among those that occurred most frequently,
- the most likely threats among those that caused the greatest losses,
- the most likely threats among those that have not occurred so far,
- the most likely threats among those that have occurred recently,
- threats causing the greatest possible losses among those that have occurred most frequently,
- threats causing the greatest possible losses among those that have caused the greatest losses,
- threats causing the greatest possible losses among those that have not emerged so far,
- threats causing the greatest possible losses among those that have occurred recently,
- threats with the greatest risk of occurrence among those that have occurred most frequently,
- threats with the greatest risk of occurrence among those that caused the greatest losses,
- threats with the greatest risk of occurrence among those that have not emerged so far,
- threats with the greatest risk of occurrence among those that have occurred recently.

3. Optimizing the choice of strategy

Let *E* denote the number of possible strategies for safeguard implementation that an organization can apply. The strategies are numbered from 1 to *E*. Let *N* indicate the number of global measures that the organization takes into account when assessing the safeguard implementation strategy. Let $R_n^e \in \mathbb{Y}_n$ be a global measure n, obtained by applying the strategy e and random variables describing threat occurrence, where $\mathbb{Y}_n$ is a set of random variables with values from the $\overline{\mathbb{Y}}_n$ set, describing global measures. Let $\overline{R}_n^e\left(\overline{\mathbb{X}}(1), ..., \overline{\mathbb{X}}(T)\right) \in \overline{\mathbb{Y}}$ be the value of this measure for threats described by $\overline{\mathbb{X}}(1), ..., \overline{\mathbb{X}}(T)$. Let $R_n^{opt}\left(\overline{\mathbb{X}}(1), ..., \overline{\mathbb{X}}(T)\right)$ indicate the optimum value for the global measure n, i.e. the value of a global measure assuming full knowledge of the process of threat occurrence described by $\overline{\mathbb{X}}(1), ..., \overline{\mathbb{X}}(T)$ and implementation of the best set of safeguards.

When taking into account several global measures simultaneously, the choice of the optimal strategy needs to account for polyoptimization. The relevant tasks can therefore be analyzed using a rich set of multicriteria optimization methods. Below, we list a few approaches equivalent to the ideal point method. An optimization task involving the choice of the optimal strategy can be formulated as follows:

For known variables: *E*, *N*, *T*, $\mathbb{X} = \left\langle X_1, X_2, \ldots, X_V \right\rangle$ – the vector of discrete random variables with values from the $\overline{\mathbb{X}}$ set,

$$\left\{\left[\overline{R}_n^e\left(\mathbb{X}(1),\ldots,\overline{\mathbb{X}}(T)\right)\right]_{E\times N}\right\}_{\left\langle\overline{\mathbb{X}}(1),\ldots,\overline{\mathbb{X}}(T)\right\rangle\in\overline{\mathbb{X}}},$$

$$\left\{\left[R_n^{opt}\left(\overline{\mathbb{X}}(1),\ldots,\overline{\mathbb{X}}(T)\right)\right]_{E\times N}\right\}_{\left\langle\overline{\mathbb{X}}(1),\ldots,\overline{\mathbb{X}}(T)\right\rangle\in\overline{\mathbb{X}}}$$

determine:

$e^* \in \{1,\ldots,\mathrm{E}\}$, that is the strategy the organization is to implement so as to:

$$f\left(e^*\right) = \min_{e\in\{1,\ldots,E\}} \sum_{\left\langle\overline{\mathbb{X}}(1),\ldots,\overline{\mathbb{X}}(T)\right\rangle\in\overline{\mathbb{X}}} \left\|\left\langle R_1^{opt}\left(\overline{\mathbb{X}}(1),\ldots,\overline{\mathbb{X}}(T)\right),\ldots\right.\right.$$

$$\ldots, R_N^{opt}\left(\overline{\mathbb{X}}(1),\ldots,\overline{\mathbb{X}}(T)\right)\Big\rangle - \Big\langle\overline{R}_1^e\left(\overline{\mathbb{X}}(1),\ldots,\overline{\mathbb{X}}(T)\right),\ldots$$

$$\left.\left.\ldots,\overline{R}_N^e\left(\overline{\mathbb{X}}(1),\ldots,\overline{\mathbb{X}}(T)\right)\right\rangle\right\|\cdot$$

$$\cdot\mathcal{Pr}\left\{<\underbrace{\mathbb{X},\ldots,\mathbb{X}}_{T}>=\left\langle\overline{\mathbb{X}}(1),\ldots,\overline{\mathbb{X}}(T)\right\rangle\right\}$$

where $\|\bullet\|$ is the norm in the criterion space of the polyoptimization task.

In this task, point $\left[R_n^{opt}\left(\overline{\mathbb{X}}(1),\ldots,\overline{\mathbb{X}}(T)\right)\right]_N \in \Re^N$ is the ideal point, and

$$\left\|\left\langle R_1^{opt}\left(\overline{\mathbb{X}}(1),\ldots,\overline{\mathbb{X}}(T)\right),\ldots,R_N^{opt}\left(\overline{\mathbb{X}}(1),\ldots,\overline{\mathbb{X}}(T)\right)\right\rangle - \right. \\ \left. -\left\langle\overline{R}_1^e\left(\overline{\mathbb{X}}(1),\ldots,\overline{\mathbb{X}}(T)\right),\ldots,\overline{R}_N^e\left(\overline{\mathbb{X}}(1),\ldots,\overline{\mathbb{X}}(T)\right)\right\rangle\right\| \tag{10}$$

is the distance of the vector of realization of random variables $\left\langle R_1^e,\ldots,R_N^e\right\rangle$ from the ideal point.

Due to the complexity of the task it is impossible to apply analytical methods to find a generalized solution. Therefore, a simulation method is suggested to complete the optimization task. It assumes carrying out simulation experiments, each of which is conducted as follows:

1. The $\overline{X_v}(t)$ values are drawn on the basis of X_v random variables.
2. Global measures values for all strategies are calculated as realizations of random variables $R_n^e \in \mathbb{Y}_n$.
3. The optimum values of metrics are calculated $\left[R_n^{opt}\left(\overline{\mathbf{X}}(1),\ldots,\overline{\mathbf{X}}(T)\right)\right]_N \in \Re^N$ (e.g. using dynamic programming [1]) as a realization of random variables for the same threats, but with the best method of counteraction.
4. The values of the objective function are calculated as the average of the norm values for each strategy.
5. A strategy for which the above figures are the lowest is determined as optimal.

On the basis of all simulations, the strategy to be chosen is the one which achieves average results closest to the considered ideal points. The number of simulation experiments should be established using methods of examining the adequacy of simulation experiments to the random variables. Assuming that we have the knowledge about the distributions of the degree of the occurrence of real threats and of threats observed during the simulation experiments, one can perform appropriate credibility tests of the obtained results, e.g. using a compatibility test (chi-square) [9], and on that basis determine the required number of simulation experiments.

Implementation of the suggested method should be performed as follows:

1. The context is set, business processes, threats and safeguards are identified. At this stage the function of financial loss for each business process is determined. It takes into account the impact of threats and the impact of safeguard application.
2. A budget for implementing and maintaining safeguards is determined. The organization determines what amount of funding is to be spent on implementing and maintaining safeguards.
3. The organization decides about acceptable strategies that can be applied.
4. The safeguard strategy evaluation function is described (e.g. based on selected measures). The organization makes a decision as to on what metrics and statistics the selected strategy will be based and how many simulation experiments need to be carried out.
5. Simulation experiments are conducted and selected strategies are evaluated based on the values of global measures and optimal values of global measures.
6. If the results are satisfactory for the organization, the optimal strategy is selected. Otherwise, the process starts again from establishing the budget for the implementation and maintenance of safeguards (e.g. safeguard funding may be changed).

4. Sample business case

The following scenario presents a case in which the organization makes decisions about the choice of the optimal strategy from a set of acceptable strategies:

- “The most expensive”. This strategy belongs to a group of strategies independent of threat history and independent of threat anticipation. It assumes implementing in each time period safeguards of the maximum permissible total implementation and maintenance costs and hoping that such protection will be most effective.
- “Stay ahead of threats with the greatest risk of occurrence”. This strategy belongs to a group of strategies independent of threat history and dependent on threat anticipation. It is an attempt to protect the organization against those threats whose consequences are large, and which are highly likely to occur.

For the purpose of selecting the optimal strategy in the above scenario two global measures are chosen. The first selected measure is the organization’s budget $\Gamma\left(T,\mathbb{S}\right)$ described by means of recursion:

$$\Gamma\left(0,\mathbb{S}\right)=\Gamma_0;$$

$$\begin{aligned}\Gamma\left(t,\mathbb{S}\right)&=\Gamma\left(t-1,\mathbb{S}\right)+\sum_{p=1}^{P}L_p\left(t\right)-\\&-\sum_{p=1}^{P}\Phi_p\left(\mathcal{X}\left(t\right),\mathbb{S}\right)-\\&-\sum_{p=1}^{P}\sum_{i=1}^{I}\overline{O}_i\sum_{n=1}^{t}s_i\left(n\right)\cdot e_i^p\left(n,t\right)\ \text{ for }\ t=\overline{1,T}\end{aligned}\tag{11}$$

A symbol used in this formula $\left[\varphi\right]\in\left\{0,1\right\}$ is the Iverson’s bracket, where φ is a statement that can be true or false.

This measure was chosen because most often the main purpose of a business organization is to obtain the largest budget at the end of the analyzed time period.

The second measure is $\Lambda\left(\mathrm{T},\mathbb{S}\right)$ – the number of threats that brought a loss in the analyzed time period, denoted by:

$$\Lambda\left(\mathrm{T},\mathbb{S}\right)=\\=\sum_{n=1}^{T}\sum_{v=1}^{V}\operatorname{sgn}\left(\sum_{p=1}^{P}\Phi_p\left(\begin{bmatrix}X_1\left(1\right)&\cdots&&X_v\left(1\right)&&\cdots&X_V\left(1\right)\\\vdots&\vdots&&\vdots&&\vdots&\vdots\\X_1\left(t-1\right)&&&X_v\left(t-1\right)&&&X_V\left(t-1\right)\\0&\cdots&0&X_v\left(t\right)&0&\cdots&0\\0&\cdots&&0&&\cdots&0\\\vdots&\vdots&&\vdots&&\vdots&\vdots\\0&\cdots&&0&&\cdots&0\end{bmatrix}_{V\times T},\mathbb{S}\right)\right)\tag{12}$$

Based on this measurement, a modern business organization is able to juxtapose its results against the results of organizations similar as regards, i.e. the type of activity, area of operation, number of employees, etc. (Benchmarking [3]).

For the purpose of choosing the optimal strategy in line with the concept of the ideal point, the values of global measures were standardized. The need for normalization stems from the diversity of labels assigned to different criteria and different absolute values of these criteria. Therefore, some normalization was introduced to dimensionless quantities from the $\left[0,1\right]$ range, with reference to extreme values of the measures in question.

Normalization of $\Gamma\left(T,\mathbb{S}\right)$ measurement is carried out using the min-max normalization function. Let $\Gamma\left(T,\mathbb{S}\right)_{\max}\in\mathbb{R}$ mean a best-case scenario budget, with no threats at any time period, that is $\forall v=\overline{1,V};\forall t=\overline{1,T}:X_v\left(t\right)=0$, and an organization which has not commenced safeguard implementation in any time period, thus not incurring any costs, that is $\forall i=\overline{1,I};\forall t=\overline{1,T}:s_i\left(t\right)=0$. The $\Gamma\left(T,\mathbb{S}\right)_{\max}$ value is denoted by: $\Gamma\left(T,\mathbb{S}\right)_{\max}=\sum_{p=1}^{P}\sum_{t=1}^{T}L_p\left(t\right)$.

Let $\Gamma\left(T,\mathbb{S}\right)_{\min}\in\mathbb{R}$ mean a worst-case scenario budget where each threat occurred in each time period with maximum intensity, that is $\forall v=\overline{1,V};\forall t=\overline{1,T}:X_v\left(t\right)=\max\mathbb{X}_v$, and the organization has not commenced safeguard implementation in any time period, that is $\forall i=\overline{1,I};\forall t=\overline{1,T}:s_i\left(t\right)=0$. The $\Gamma\left(T,\mathbb{S}\right)_{\min}$ value is denoted by:

$$\Gamma\left(T,\mathbb{S}\right)_{\min}=\sum_{p=1}^{P}\sum_{t=1}^{T}L_p\left(t\right)-\\-\sum_{p=1}^{P}\sum_{t=1}^{T}\Phi_p\left(\begin{bmatrix}\max\overline{\mathbb{X}}_1&\ldots&\max\overline{\mathbb{X}}_V\\\ldots&\max\overline{\mathbb{X}}_v&\ldots\\\max\overline{\mathbb{X}}_1&\ldots&\max\overline{\mathbb{X}}_V\end{bmatrix}_{V\times T},\begin{bmatrix}0&\ldots&0\\\ldots&0&\ldots\\0&\ldots&0\end{bmatrix}_{I\times T}\right)$$

Let $\hat{\Gamma}\left(T,\mathbb{S}\right)\in\mathbb{R}$ mean the budget the organization obtained at the end of the analyzed time period, normalized to $\left[0,1\right]$ range. In this case $\hat{\Gamma}\left(T,\mathbb{S}\right)$ is denoted by:

$$\begin{aligned}\hat{\Gamma}\left(T,\mathbb{S}\right)&=\frac{\Gamma\left(T,\mathbb{S}\right)-\Gamma\left(T,\mathbb{S}\right)_{\min}}{\Gamma\left(T,\mathbb{S}\right)_{\max}-\Gamma\left(T,\mathbb{S}\right)_{\min}}\\&=\frac{\Gamma\left(T,\mathbb{S}\right)-\Gamma\left(T,\mathbb{S}\right)_{\min}}{\sum_{p=1}^{P}\sum_{t=1}^{T}L_p\left(t\right)-\Gamma\left(T,\mathbb{S}\right)_{\min}}\end{aligned}\tag{13}$$

The normalization of the $\Lambda\left(T,\mathbb{S}\right)$ measure is carried out using the min-max normalization function. Let $\Lambda\left(T,\mathbb{S}\right)_{\max}\in\mathbb{P}$ mean the number of threats causing losses in the worst-case scenario where each treat occurred in each time period, that is $\forall v=\overline{1,V};\forall t=\overline{1,T}:\overline{X_v}\left(t\right)>0$, and the organization has not commenced safeguard implementation in any time period, that is $\forall i=\overline{1,I};\forall t=\overline{1,T}:s_i\left(t\right)=0$. The $\Lambda\left(T,\mathbb{S}\right)_{\max}$ value is denoted by: $\Lambda\left(T,\mathbb{S}\right)_{\max}=V\cdot T$.

Let $\Lambda\left(T,\mathbb{S}\right)_{\min}\in\mathbb{P}$ mean the number of threats causing losses in the best-case scenario with no threats at any time period, that is $\forall v=\overline{1,V};\forall t=\overline{1,T}:\overline{X_v}\left(t\right)=0$. In this case $\Lambda\left(T,\mathbb{S}\right)_{\min}=0$. Let $\widehat{\Lambda}\left(T,\mathbb{S}\right)$ mean the number of threats that occurred and caused loss in the analyzed time period, normalized to $\left[0,1\right]$ range. Thus $\widehat{\Lambda}\left(T,\mathbb{S}\right)$ is denoted by:

$$\widehat{\Lambda}\left(T,\mathbb{S}\right)=\frac{\Lambda\left(T,\mathbb{S}\right)-\Lambda\left(T,\mathbb{S}\right)_{\min}}{\Lambda\left(T,\mathbb{S}\right)_{\max}-\Lambda\left(T,\mathbb{S}\right)_{\min}}=\frac{\Lambda\left(T,\mathbb{S}\right)}{V\cdot T} \qquad (14)$$

In the following scenario, the occurrence of threats in each time period is equally probable; the possible occurrence of one of the threats will not cause big losses, but the occurrence of other threats can lead to large losses. The organization cannot begin the implementation of all safeguards at the beginning of the analyzed time period, because its budget does not allow this.

The organization runs a business process involving the import of fees for insurance policies. The process brings financial effect of $L_1\left(t\right)=30000$ in each time period. The financial limit for implementing and maintaining safeguards equals

$$\overline{\Gamma}\left(t\right)=\begin{cases}150 \text{ for } t=1\\ 0 \text{ for } t>1\end{cases}$$

. The analyzed time period is divided into $T=12$ sub-periods. During that period, the following threats may occur:

1. Number 1: a power outage, with the degree of probability as below:
   $\mathcal{P}r\left\{X_1\left(t\right)=0\right\}=0.906$
   $\mathcal{P}r\left\{X_1\left(t\right)=1\right\}=0.094$
2. Number 2: application server failure, with the degree of probability as below:
   $\mathcal{P}r\left\{X_2\left(t\right)=0\right\}=0.906$
   $\mathcal{P}r\left\{X_2\left(t\right)=1\right\}=0.094$
3. Number 3: database server failure, with the degree of probability as below:
   $\mathcal{P}r\left\{X_3\left(t\right)=0\right\}=0.910$
   $\mathcal{P}r\left\{X_3\left(t\right)=1\right\}=0.090$
4. Number 4: unannounced system operator absence, with the degree of probability as below:
   $\mathcal{P}r\left\{X_4\left(t\right)=0\right\}=0.910$
   $\mathcal{P}r\left\{X_4\left(t\right)=1\right\}=0.090$

The number of possible safeguards $I=4$. Possible safeguards comprise:

1. Number 1: UPS with $\overline{O_1}=1$ intensity; time of implementation is independent of the time period in which implementation starts and amounts to $G_1\left(t\right)=1$; time of usefulness is independent of the time period in which implementation starts and amounts to $r_1\left(t\right)=8$. The cost of this safeguard is borne only at the beginning of its implementation and equals the cost of purchase, i.e. 110.
2. Number 2: a backup application server with $\overline{O_2}=1$ intensity; time of implementation is independent of the time period in which the implementation starts and amounts to $G_2\left(t\right)=1$; time of usefulness is independent of the time period in which the implementation starts and amounts to $r_2\left(t\right)=9$. The cost of this safeguard is borne only at the beginning of its implementation and equals the cost of purchase, i.e. 130.
3. Number 3: a backup database server with $\overline{O_3}=1$intensity; time of implementation is independent of the time period in which the implementation starts and amounts to $G_3\left(t\right)=1$; time of usefulness is independent of the time period in which the implementation starts and amounts to $r_3\left(t\right)=8$. The cost of this safeguard is borne only at the beginning of its implementation and equals the cost of purchase, i.e. 120.
4. Number 4: training of a second system operator with $\overline{O_4}=1$ intensity; time of implementation is independent of the time period in which the implementation starts and amounts to $G_4\left(t\right)=1$; time of usefulness independent of the time period in which the implementation starts amounts to

$r_4(t) = 8$. The cost of this safeguard is borne only at the beginning of its implementation and equals the cost of purchase, i.e. 150.

The safeguards are not mutually exclusive neither during their implementation nor during their functioning. In the initial stage there are no operating or implemented safeguards. The financial loss for the business process in time period t is denoted by:

$$\begin{aligned}
&\Phi_1(\mathcal{X}(t), \mathbb{S}) = 3080 \cdot X_1(t) - 3080 \cdot \operatorname{sgn}(X_1(t)) \cdot \sum_{u=1}^{t} s_1(u) \cdot \\
&\cdot [u + G_1(u) \le t < \min\{T, u + G_1(u) + r_1(u)\}] + \\
&+3035 \cdot X_2(t) - 3035 \cdot \operatorname{sgn}(X_2(t)) \cdot \\
&\cdot \sum_{u=1}^{t} s_2(u) \cdot [u + G_2(u) \le t \min\{T, u + G_2(u) + r_2(u)\}] + \\
&+3100 \cdot X_3(t) - 3100 \cdot \operatorname{sgn}(X_3(t)) \cdot \\
&\cdot \sum_{u=1}^{t} s_3(u) \cdot [u + G_3(u) \le t < \min\{T, u + G_3(u) + r_3(u)\}] + \\
&+150 \cdot X_4(t) - 140 \cdot \operatorname{sgn}(X_4(t)) \cdot \\
&\cdot \sum_{u=1}^{t} s_4(u) \cdot [u + G_4(u) \le t < \min\{T, u + G_4(u) + r_4(u)\}]
\end{aligned}$$

For each strategy in the analyzed scenario global measures calculated in subsequent simulation experiments are presented in the table below.

Tab. 1. Global measures values

Simulation number	Global measure	The most expensive	Stay ahead of threats with the greatest risk of occurrence	Optimal solution
1	$\Gamma(T, \mathbb{S})$	350635	353690	353765
	$\Lambda(T, \mathbb{S})$	3	2	2
2	$\Gamma(T, \mathbb{S})$	359850	359870	360000
	$\Lambda(T, \mathbb{S})$	0	0	0
3	$\Gamma(T, \mathbb{S})$	350700	353755	353755
	$\Lambda(T, \mathbb{S})$	3	2	2
4	$\Gamma(T, \mathbb{S})$	359850	359870	360000
	$\Lambda(T, \mathbb{S})$	0	0	0
5	$\Gamma(T, \mathbb{S})$	338215	341270	344305
	$\Lambda(T, \mathbb{S})$	8	7	6
6	$\Gamma(T, \mathbb{S})$	350485	350505	353615
	$\Lambda(T, \mathbb{S})$	4	4	3
7	$\Gamma(T, \mathbb{S})$	350635	353690	353765
	$\Lambda(T, \mathbb{S})$	3	2	2
8	$\Gamma(T, \mathbb{S})$	350635	353690	353765
	$\Lambda(T, \mathbb{S})$	3	2	2
9	$\Gamma(T, \mathbb{S})$	350635	353690	353765
	$\Lambda(T, \mathbb{S})$	3	2	2
10	$\Gamma(T, \mathbb{S})$	341420	347510	347650
	$\Lambda(T, \mathbb{S})$	6	4	4

The normalized global measures values calculated in the above experiments for each simulation strategy are presented in the table below.

Tab. 2. Normalized global measures values

Simulation number	Global measure	The most expensive	Stay ahead of threats with the greatest risk of occurrence	Optimal solution
1	$\hat{\Gamma}(T, \mathbb{S})$	0.9167	0.9444	0.9445
	$\hat{\Lambda}(T, \mathbb{S})$	0.0625	0.0417	0.0417
2	$\hat{\Gamma}(T, \mathbb{S})$	0.9987	0.9990	1.0000
	$\hat{\Lambda}(T, \mathbb{S})$	0.0000	0.0000	0.0000
3	$\hat{\Gamma}(T, \mathbb{S})$	0.9172	0.9176	0.9444
	$\hat{\Lambda}(T, \mathbb{S})$	0.0625	0.0625	0.0417
4	$\hat{\Gamma}(T, \mathbb{S})$	0.9987	0.9990	1.0000
	$\hat{\Lambda}(T, \mathbb{S})$	0.0000	0.0000	0.0000
5	$\hat{\Gamma}(T, \mathbb{S})$	0.8061	0.8339	0.8603
	$\hat{\Lambda}(T, \mathbb{S})$	0.1667	0.1458	0.1250
6	$\hat{\Gamma}(T, \mathbb{S})$	0.9153	0.9157	0.9432
	$\hat{\Lambda}(T, \mathbb{S})$	0.0833	0.0833	0.0625
7	$\hat{\Gamma}(T, \mathbb{S})$	0.9167	0.9444	0.9445
	$\hat{\Lambda}(T, \mathbb{S})$	0.0625	0.0417	0.0417
8	$\hat{\Gamma}(T, \mathbb{S})$	0.9167	0.9444	0.9445
	$\hat{\Lambda}(T, \mathbb{S})$	0.0625	0.0417	0.0417
9	$\hat{\Gamma}(T, \mathbb{S})$	0.9167	0.9444	0.9445
	$\hat{\Lambda}(T, \mathbb{S})$	0.0625	0.0417	0.0417
10	$\hat{\Gamma}(T, \mathbb{S})$	0.8347	0.8898	0.8901
	$\hat{\Lambda}(T, \mathbb{S})$	0.1250	0.0833	0.0833

The norm (10) with $p = 2$ parameter are presented in the table below.

Tab. 3. Norm with p = 2 parameter

Simulation number	The most expensive	Stay ahead of threats with the greatest risk of occurrence
1	0.0348	0.0001
2	0.0013	0.0010
3	0.0342	0.0340
4	0.0013	0.0010
5	0.0684	0.0337
6	0.0348	0.0345
7	0.0348	0.0001
8	0.0348	0.0001
9	0.0348	0.0001
10	0.0310	0.0116
Average	0.0349	0.0105

Based on the simulations, the organization should choose the strategy labeled as "Stay ahead of threats with the greatest risk of occurrence".

5. Conclusions

Modern organizations face a difficult decision when choosing safeguard management strategies. They need to account for the individual requirements, analyze the level of threat occurrence, and estimate possible financial losses. There is no reason not to apply hybrid strategies, e.g. use the "most expensive" strategy for the first few time periods, then the "stay ahead of threats with the greatest risk of occurrence" strategy and in the final phase the "nothing to implement" strategy. Any strategy can be analyzed in the same manner as the strategies discussed above.

The organization should determine:

- the range of permissible strategies,
- global measures that will be used to evaluate the strategies,
- way of selecting the optimal strategy in the case of the use of a number of global measures based on simulation experiments,
- the number of simulation experiments (the more experiments, the higher the reliability of the results obtained, but the longer the simulation).

6. Bibliography

[1] Bellman R., *The theory of dynamic programming*, Rand Corporation, Santa Monica, 1954.

[2] Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, WNT, Warsaw, 2006.

[3] Bogetoft P., *Performance Benchmarking*, Springer, New York, 2012.

[4] Chojnacki A., *Modelowanie matematyczne*, WAT, Warsaw, 1986.

[5] Chojnacki A., Pieniążek G., "Time based deterministic model of information security of a business organization", *Computer Science and Mathematical Modelling*, No. 1, 17–24 (2015).

[6] Flasiński M., *Zarządzanie projektami informatycznymi*, PWN, Warsaw, 2006.

[7] Oberlander G.D., *Project Management for Engineering and Construction*, McGraw--Hill, Boston, 2000.

[8] Pieniążek G., Zaskórski P., "Modelowanie systemów biznesowych z uwzględnieniem wartościowania bezpieczeństwa informacyjnego organizacji", in: *Nowoczesne systemy zarządzania*, Włodzimierz Miszalski (Eds.), 237–250, WAT, Warsaw, 2011.

[9] Rothock L., Narayanan S., *Human-in-the-LoopSimulations*, Springer, London, 2011.

[10] Trocki M., Grucza B., Ogonek K., *Zarządzanie projektami*, PWE, Warsaw, 2009.

[11] Zaskórski P., Pieniążek G., "Information security criteria in the design of business systems", in: *Studia Bezpieczeństwa narodowego*, Bogusław Jagusiak (Eds.), 91–107, WAT, Warsaw, 2011.

[12] Zaskórski P., Pieniążek G., "Ciągłość działania organizacji w warunkach asymetrii informacyjnej", in: *Zarządzanie kryzysowe – różne oblicza*, Romuald Grocki (Eds.), 37–51, Wydawnictwo Dolnośląskiej Wyższej Szkoły Służb Publicznych ASESOR, Wrocław 2010.

Metoda symulacyjna wyboru optymalnej strategii bezpieczeństwa informacyjnego w organizacji biznesowej

A. CHOJNACKI, G. PIENIĄŻEK

W artykule opisano strategie wdrażania zabezpieczeń w organizacji biznesowej. Strategie są sklasyfikowane w grupy według zależności od historii występowania zagrożeń oraz zależności od historii wdrażanych zabezpieczeń. Następnie przedstawiona jest metoda wyboru optymalnej strategii dla organizacji biznesowej, przy ustalonym kontekście. W kolejnym kroku wprowadzona metoda jest użyta do wyboru optymalnej strategii w przykładowym przypadku biznesowym. Metoda bazuje na deterministycznym, czasowym modelu bezpieczeństwa informacyjnego, który został rozszerzony do modelu losowego. Dzięki metodzie symulacyjnej organizacja może wybrać najlepszą, dla siebie, strategię wdrażania zabezpieczeń. Jest to istotne we współczesnych organizacjach, aby przeprowadzić analizę kosztów i ryzyka, w celu doboru odpowiednich zabezpieczeń.

Słowa kluczowe: bezpieczeństwo informacyjne, symulacja, strategia.