Journal scientific and applied research, vol. 6, 2014
Association Scientific and Applied Research
International Journal

Original Contribution

ISSN 1314-6289

A PASSIVE STRATEGY FOR MANAGEMENT OF COUNTERACTION TO ENCROACHMENTS ON BUSINESS ORGANIZATION

Hristo Hristov

SHUMEN UNIVERSITY "BISHOP KONSTANTIN PRESLAVSKI"
E-mail: *hristov63@abv.bg*

Abstract: *From the point of view of one social organization a rational choice about an alternative for an action in a definite security environment is made on the basis of defining optimum of possible numbers of alternatives among which a choice is being fulfilled towards putting into practice a system of criteria in order to compare options of alternatives. For that reason taking a decision connected with a choice about a strategy for management of counteraction to encroachments on social organization is one of the most difficult management tasks that has ever been carried out on the circumstances of complex and dynamic fast-changing security environment.*

Key words: *company security environment, strategies about security, active and passive strategies, security environment, security environment, management, business organization, protection, encroachments, counteraction.*

From the point of view of one social organization a rational choice about an alternative for an action in a definite security environment is made on the basis of defining optimum of possible numbers of alternatives among which a choice about putting into practice a system of criteria in order to compare options of alternatives is being fulfilled. For that reason, taking a decision connected with a choice about a strategy for management of counteraction to encroachments on social organization is one of the most difficult management tasks that has ever been carried out on the circumstances of complex and dynamic fast-changing security environment.

Theoretical directions about four levels of strategy's choice in critical situations or in situations in which the system seeks to take control under risks' factors that are able to bring destabilization to system's management as well as to drain its material, financial, cognitive (related to knowledge) and human resources and to increase its security are [1]:

The first level (H1) is ,,doing something''. In this case there isn't any strategy but just a reaction to environment, influences, impulses, the behavior adapts to risks, problems, tasks and difficulties.

The second level (H2) is ,,having a strategy is better than the lack of strategy''. In this case the organization works out and abides by one behavior strategy whatever it may be.

The third level (H3) is ,,the best strategy is better than the other strategies''. In this case organization elaborates several strategies and picks up the best one on the basis of definite sets of criteria.

The fourth level (H4) is ,,extending the context''. In this case the best strategy among all single-handedly worked out and applied strategies leads nowhere so the system should seek and apply another strategy or accede to someone's other successful strategy.

The whole process of counteraction management like each management process is a constant round of taking decisions and a permanent search for solutions of problems by different nature.

Taking a decision in the circumstances of non-linearity and chaotic state is never-stopping process aimed to decrease the state of chaos for one system.

The decision is making a choice among alternatives for actions at the time when definite objectives are being realized. The decision is made by management teams on different management levels who are well-skilled, highly-experienced, heralds of many competencies, creative thinking and an intuition and main purpose of their activity is ,,precisely assessment of alternatives and realizing a choice in terms of organization represented by them''[2].

According to Peter Dracker ,,Whatever the manager does, it has been done through taking the decisions''. They may seem as a part of routine or concern the future existence of organization and require years to systematize them. Management is always a process about taking decisions''[3].

According to James H. Donnelly ,,The quality of management decisions is a criterion for their effectiveness and importance for the organization. Do they like or not the appraisal of their work, the remuneration of the managers is on the basis of importance, number and results of their decisions''[4].

The counteraction strategies to encroachments are scientifically supported and analytically backed with arguments and they are realized by contiguous and systematical application of mechanisms and procedures for protection and control, aimed at limiting the negative impact of existing threats and encroachments.

This study is examining mainly the passive strategy for management of counteraction to encroachments on company security so called a strategy for internal security [5].

The passive strategy for management of counteraction stands up for traditional methods of physical and personal protection. The passive strategy is working mainly in inward environment. Inward environment means those

organizational and cadres' parameters that are inherent in company – corporate traditions, culture of workplace, ethic principles, a level of managers' and executives' professionalism, coactivity between particular structural units, the physical location of objects for defense, cultural tradition and the attitude of the personnel toward problems concerning security and so on.

The performance of each operational task through the passive strategy starts with survey about conditions of security and to what extent the statute position is up to the requirement of oncoming changes outside and inside the company. After that an evaluation of vulnerability is made in terms of competitors' attacks. The next is planning the activities for neutralization that are depending on the conclusions of the evaluation. After applying the new measures for increasing the security level, the results should be reported to the Head of security service. He assesses their effectiveness and to what extent the given tasks may be accepted as well-done on that particular stage. That is the first stage of feed-back and it is realized within the framework of the service itself.

After his appraisal, the Head of the security service should report to the high management on fulfilled task. On the other hand high management weighs up the quantity of performance and to what extent the new requirements concerning internal security are applicable and are not obstacles to technical processes of particular structural units. Depending on practical results in time after a period the management is waiting for security services' evaluation in terms of which new requirements should be demanded in this particular sphere and this is the essential stage of feed-back in passive cycle. As a rule, requirements and initiatives for improving the inward security parameters should be launched by the security service not the management.

The passive strategy is carried out by a mixture of activities for revealing and counteracting to an espionage and unfair competition, detecting not allowed access to official secret, laying out company in-house order and excellent job with the staff.

The criteria and signs of detecting and counteracting to industrial espionage are considered on these lines: usage of special means of reconnaissance, acquiring or using an information from the informational massifs, breaking into company's premises, stealth of technologies, commodities, properties, money, valuables etc.; destroying or damaging the company property, sabotaging or embarrassing the technological process of the company, unfairly draw strategic supplier, buyer or other partner aside.

The protection of espionage made by deregulated usage of special means of reconnaissance may be thoroughly divided into two groups:

a) the protection with technical devices for revealing and neutralizing alien means of reconnaissance (an active defense);

b) the protection with technical devices for disrupting the routine work of special alien means of reconnaissance (a passive defense);

The passive strategy involves mounting and operation-exploitation of technical devices that hinder the normal functioning of special alien means of reconnaissance used for secret control. The last ones do not cease working; the result is only a temporary prevention from unfair competition through having an opportunity referring to unfair competition of gaining information from controlled informational environment or a communication channel.

The protection from wireless microphone tapping. The most famous method for counteracting to wireless microphone in a closed premise is an installation of device for producing rustling and thudding or setting a full radio-electronic shielding in a premise or even on the whole floor or in the particular building. Another effective method for detecting the wireless microphone is keeping watch and ward over the vicinity of the building. Revealing (the exact location) and neutralizing the wireless microphone.

To protect from the wire microphone tapping a special cable is stretched to the next-door premise that in most cases is rent by the personnel of unfair competition.

According to the passive protection from the laser directional microphone tapping the surface of glasses is made in a special technological way.

The protection from wire telephony tapping (an ordinary phone communication) is realized by an installation of device that simulates the hanged-up phone when you actually pick up the receiver (the plugged-in overloading of the voltage is averted). By this means, the tapping device of the unfair competitor stays off. This kind of method is not working when the tapping device could be switched on automatically by a timer or an outside supplying signal.

The installation of an encoding device called scrambler is also an effective method. It's possible to decode and tap the coded phone call through scrambler combined with microphone tapping of the premise, where the particular conversation is carried on.

There are devices that after a mounting in the phone line give a signal to the talker for phone tapping.

The rule for mobile phone's protection from tapping is not to make a call in the premise if you have no guarantee for its protection from microphone tapping. The unfair competitor makes a record simultaneously of your voice on the phone and coded phone signal on the radio direction finder. The next step is an easy decoding of the phone call on the principle of congruence between sound-signal and signals produced by radio-frequency.

The protection from recording a confidential call by a dictaphone is extremely difficult to be detected by technical devices and the passive defense against it has not discovered yet.

Finding, ceasing and intercepting unfair competition is possible when it's in the subsystem of inside security through two groups of methods – methods for eliminating and methods for intercepting unfair competition. The last ones as

it has been already explained include finding out and deactivating the special means of reconnaissance of an unfair competitor.

The difference between ceasing and intercepting is that the first one is characterized by denial to unfair competition deliberately made by the initiator himself. The second one – intercepting unfair competition is not of the initiator's will.

Stopping unfair competition means activities done by the counter-espionage of the affected company that provokes fear from occurring damaging consequences till the initiator has the personal motive for ceasing the unfair competition.

On the other hand intercepting unfair competition is not depending on the initiator's will. He continues willing its prolongation but outside factors are responsible for its stopping. The ceasing should be provoked by the acts of the affected security structure otherwise we can't define it as an interception.

One element of the passive strategy is the company secret and its protection. In broad terms the company secret means an information (management, production, trade, R& D, financial and business) that is not the state secret but it is chosen and included in a list by the owner/ owners and it's extra guarded. According to this definition there are some important conditions that make the difference between the company security and the other types of information: it's not the state secret; it's chosen and written in a list by the owner/ owners; there is an established method for its creating, using, preserving, destroying, controlling and guarding.

The list of reports, the facts and the subjects that are the company secret should advisably have several systemized patterns for specifying the company secret: *Information about production, Management, Plans, Finances, Market, Business partners, Negotiations, Contracts, Price, Tenders, Science and technic, Technologies, Conferences.*

After the expiry of that document, containing the company secret the precautionary stamp must be striked off and the materials should be preserved in accepted work order established by the company. Naming the people from the company staff as authorized to know and use the company security by rights (a restricted regime) has some specifics but the most important of them is interconnection between authorized staff to company secret and disciplinary or other responsibility that they should bear if there are breaches. This duty is documented by an annex of the labour agreement or by special contract. At the end the list of approved (authorized) staff attains normative power through the written order of the company manager that is only accessible to the members of manager team as well as authorized workers to company secret staff.

Creating the subsystem for information security of the company that is a part of company security system. It is designed for ensuring the execution of state and company-registered normative documents' requirements concerning the company secret through the protection of data and resources from deliberate

or incident revealing, modification, illegal usage or destroying. The scope is disseminating its influence to all levels and units of the system as well as consumers. The objects for defense are work premises, functioning stations and servers, programme and information supply, communication environment, cryptographic protection.

The subsystem for information security is designed by these main instruments: administrative resources, organizational resources, technical and programme resources.

The administrative resources contains decrees, rules and technologies concerning security and the regime of information system functioning. These instruments include functional duties of the company's officials.

Organizational resources contains measures for setting up servers, net devices, devices for encoding the info and a part of the functioning stations in the premises protected from electromagnetic radiation and controlled access.

The technic and programme resources guarantee the data protection under circumstances of global communication. The special attention here is to servers, local nets and functioning stations.

Creating this company subsystem requires execution of these activities: configuration of company intranet, determine the consumers and their rights; building a system for password management, regulating the sensible services, systematic monitoring, guarantee the entity of data, setting regulated access to data.

The main functions of the subsystem for information security are defense against electromagnetic radiation, controlling physical access, the protection for servers and functioning stations, controlling the access to resources of servers and functioning stations, protection of communication environment, total data protection, defense of working process, anti-virus protection and prophylaxis, monitoring and control.

Making practical registers refers to documental production – a mixture of concrete rules and actions and after their implementation the former-planned condition (objective) is accomplished. In this case it's the condition for maximum documents protection that contain company secret without regulated access. The company have to make instructions with normative nature, defining the documents with particular stamp, authorized staff to make documents with confidential contents, the established order for moving and using these documents.

Besides the expert is committed with teaching this method of registering the personnel.

The passive strategy includes activities related to information investigation of people, gathering facts and data for crimes, committed by the company staff, searching for missing company property, searching for missing company worker, building trustworthy relations with company personnel.

One of the basic element of the passive strategy is the work with company staff concerning matters about security that are actually talks with job applicants, instructions for new-comers in the security structure about security of preserving company data; staff training about rules of info protection, stimulating alertness inside company staff, talks with relinquishing staff, talks with the staff that break the security.

The passive strategy includes also the mixture of all requisite measures for limiting the physical access to sensitive company places (bureaus, laboratories, pay-desks) where an information with limited dissemination is saved. These measures include the following activities. Security measures with administrative function and Measures for receiving the attendants.

The effective implementation of the chosen strategy for counteraction requires also the strategic management of an organization to understand and apply the politics. It's the one responsible for strategic orientation for organization security and for creating appropriate conditions and structures for effective counteraction management.

On the basis of all said the following conclusions should be highlighted:

1. The passive strategy for counteraction management is a complex method that can be successfully used in the sphere of business security in order to reliably counteract to nowadays encroachments and threats and create one reliable security system that guarantee the execution of business organization mission.

2. Realizing the passive strategy for counteraction management in the sphere of security requires building an organizational culture for evaluating the importance of counteraction and the necessity for manage it with the efforts of the whole personnel. The strict differentiation is needed towards responsibilities for creating and implementing the politics of counteraction management and staff training that are all decisive to effective counteraction to all kinds of encroachments and threats.

3. One disadvantage of the passive strategy is that it doesn't recognize the complexity and dynamics of the changes in the security environment; proactive attitude to sources of threats is missing – striving for averting the conditions and reasons for their occurrence and manifestation, an active influence in order to oppress capabilities and motivation to a level not allowing unpleasant influence under organization and creating flexible dynamic high-technologic complex security system that guarantee the reliable organization protection that is typical for the active strategy.

Finally there is a lack of politics based on permanent aspiration for accomplishing the optimum level of information supply about processes' dynamics in social organization and security environment, about prognoses and tendencies for development of the basic environment components and sources of threats.

References:

[1] Slatinski, N., The character, meaning and containing of the security'' Military edition, http://www.vi-books.com -2011.
[2] US Naval War College, Executive Decision Making, 2002.p.15.
[3] Drucker, P., The Practice of Management, Heineman Professional Publishity, 1989. p.345.
[4] Donnelly J. and coauthors, Fundamentals of management, published in 1997, p.90.
[5] Sandev G., „Strategies for company security'', An university edition„Bishop Konstantin Preslavski'', Shumen, 2005, p.12
[6] Vasilev, Em., „Company security'', Labour, 2000.
[7] Manev Kr., Business intelligent service – the basic of cooperative security system, A symposium of scientific works – Scientific conference, National Military University „V.Levski'', The faculty „Artillery, Aircraft defense and communication information system'', Shumen, 2012.
[8] Asenov B., Kiprov, P., The theory of security service, Labour, 2000.
[9] Vasilev, Em., Company security, Labour, 2000.
[10] Sandev, G., National security, The editing house „Faber'', 2008.
[11] Sandev, G., Security of organizations, An university edition „Bishop Konstantin Preslavski'', Shumen, 2012, ISBN 978-954-577-621-2.
[12] Nachev, Jo, The competitive security service, Siela, 2007.