DEVELOPING AND MAINTAINING BUSINESS SECURITY CULTURE

Konstantin Poudin[1]

Introduction

Security is an extremely important issue. According to J. Nye, security is like oxygen: you tend not to notice it until you lose it. That is why all issues connected with it are always topical and invariably attract the attention of researchers and practitioners alike. All social systems need security to achieve their goals. Some of them are business organizations. Briefly business security means absence of threats to the interests of the business organizations. These threats come from the internal and external environment of every business.

Business security culture is a foundation of business security. It has two aspects – cognitive and behavioural. That is why security culture could be presented as a way of knowing and understanding of the things, which happen in the internal and external environment and the reaction regarding these things.

Building and maintaining security culture has a managerial aspect. The major assumption held in this paper is that each business organization should pay attention to the management of security culture, including the development and maintenance thereof, considering that security-related culture provides the basis of the business organizations' security, protection and achievement of its interests.

The topic of business security culture has not yet been given due attention on the part of the academic and research circles in Bulgaria. The goal of the current paper is to draw attention to this topic. Without claiming exhaustiveness, the study aims to shed light on the main aspects of the subject. This paper makes an attempt to perform three main tasks, namely the analysis of: 1) the business security concept; 2) the concept of business culture; 3) the development and maintenance of business security culture.

Each social system (each individual, group of people, business organization, any society or state, and even an alliance of states) has a specific security culture, which determines its attitude to the environment and the way security is guaranteed. This paper is dedicated to the security culture at the organizational level.

[1] Konstantin Poudin, PhD, Assoc. Prof., Department of National and Regional Security, email: kpoudin@unwe.bg.

The article is based on different kinds of research carried out by researchers and managers that have an interest in the field of management, business security, organizational behaviour and organizational culture etc.

This paper is targeted at to a broad readership, including entrepreneurs, researchers, students and all kind of readers who take an interest in this matter.

Thoughts on Business Security

It is a commonly held view that a business is an organizational entity involved in the provision of goods and services to consumers. It is also known as an enterprise, a company, a firm or a corporation. Roger Burlton points out that a business is an organization, the aim of which is to create valuable results for those who care about those results. (Burlton, 2001)

Having in mind the ideas outlined above, business security should be seen as pertaining to the security of enterprises (no matter of their name – a company, a firm or a corporation) that produces products and offer services on the market.

All such business organizations have goals which are based on their interests. Their main goal is to make a profit, satisfying public needs for goods and services in the desired quality and quantity, and at a reasonable price. After the concept of Impact-driven Businesses (companies, corporations) emerged, many businesses began to show their commitment to social and environmental issues as well. (NBIS, 2012, pp.1-8)

In one of his books Georgi Stefanov points out that the interests are focused on:

- getting something valuable (e.g. a starting enterprise attracts clients and gets some market share);
- protecting something valuable (e.g. the same enterprise has to keep the acquired market share in a competitive condition);
- enlarging/increasing something valuable (e.g. the same enterprise has to extend the acquired market share in a competitive condition). (Stefanov, 2008, pp. 70-71)

Nikolay Slatinski highlights that security can be defined as the measure of how a system (e.g. people, communities of people, societies, countries, communities of countries) protects its interests in the conflict, using its own power. (Slatinski, 2011, p.113) The notions system, interests, power and conflicts are the key notions in his definition (see Table 1).

Table 1. Basic Notions Defining Security

Notion	Definition
Systems	People, communities of people, societies, countries, communities of countries. [1]
Interests	Conscious needs, highly situated in the systems' scale of priorities.
Conflict	Clash, interaction between the interests of different systems.
Power	All the resources used by a system to protect its interests in the conflict.

Source: Slatinski, 2011, p. 113

In a broad sense of the term, security or state of security suggests an absence of threat to somebody's interests (getting, protecting and increasing something valuable). These threats are related to the environment – internal and external one for the given subject.

Business security means absence of threat to business interests. It is the state of the internal and the external environment in which the firm/company/corporation/organization operates, characterized by absence of threats and dangers to its interests or if there are any, the business has the ability to meet and tackle them. It could be further defined as a policy at the corporate level aimed at foreseeing and offsetting the threats to the business interests and creating conditions for the realization of business goals. In other words, business security eliminates the threats and creates opportunities.

Every business organization is a system built of subsystems – managerial, financial, HR, production, IT etc., whose functions are interrelated. In a broad sense, business security has to guarantee the normal functioning of all these subsystems, which means that business organizations can achieve their mission and goals. [2]

Business security goals could be the recognition of threats, their prevention or elimination, or creating of opportunities for normal functioning of the business. The achievement of these goals requires resources. The resources should be managed in an appropriate way and comprise financial, informational, material, human resources, to name just a few.

In their overview of the various perspectives related to resource-based view to the business, Jeroen Kraaijenbrink and Aard Groen point out that the resources are the capacities used in a business's actions. They are the means that enable and constrain the actions a firm can perform. This means that resources allow for firms to perform their actions, yet resources also constrain them in their operations. Resources gathered in the past will largely define what a firm can do and what it cannot do. Yet, new resources can be gathered that expands the scope

of possible actions. In addition to being inputs to a firm's actions, resources are also affected by these same actions. As such, they are outputs of actions as well. (Kraaijenbrink, J. and Groen, A., 2008, p. 2)

Financial resources – Money is not everything but everything is related to money. The availability of sufficient financial resources and their good management is a guarantee for bigger business stability, in ceteris paribus. Part of these resources is directly allocated for activities related to physical security, information security, and safety, as well. Other part of the resources is planned for the functional activities of the organization and in indirect way could affect organization's security. The availability of other resources for security (e.g. material resources for security – e.g. video surveillance, scanners, metal detectors etc.) depends to a large extent on the financial resources.

Information resources – Information as a resource for business security is related to different IT products, which have to protect the information assets of the business. These resources are part of Information Security Management System (ISMS) developed in many business organizations, giving them strategic advantages (Tagarev, 2011, pp. 615-621). Information resources are also associated with a specific knowledge, know-how and experience based on systematic and constant benchmarking analyses. **They are also related to the availability of reliable, complete, and on time information about the different processes in the internal and external environment that can jeopardize business organization**'s interests or allow the business to gain competitive advantages.

Material resources – Material resources include assets (most often different types of technical systems), which are used to guarantee different security aspects – physical, information, personnel or combination of them.

Human resources – This resource resides in knowledge, skills, and motivation of people. Human resource is the least mobile of the four factors of production, and (under right conditions) it improves with age and experience, which no other resource can do. It is therefore regarded as the most important and productive resource that creates the greatest and longest lasting advantage for an organization. (Business Dictionary, 2017) Business security depends primarily on human resources.

Concept of Business Security Culture

Business security culture is a subset of the culture of the business organization. Organizational culture could be defined in many ways. Due to the practical importance that organizational culture has in everyday life of each organization, it is the matter of serious research interest. Great attention is paid to clarifying its scope and its impact on the organization's activities, as well as the ways of its development and change.

Kiril Dimitrov points out three main approaches to clarify the essence of organizational culture:

- Problematic approach – It includes two main problems faced by each organization's staff: the survival and adaptation of the group to the external environment and the problem of internal integration among group members.
- Content approach – The attention is focused on making of a list of company's culture elements: organization history, founder's biography, rituals, ceremonies, myths, symbols, etc.
- Functional approach – Within this approach the focus is on the usefulness of organizational culture for different interest groups.
- Etymological approach and other important research streams, which influence the perception of the concept of organizational culture. (Dimitrov, 2012, p.11 and Dimitrov and Geshkov, 2018, p. 385)

In the context of the above-mentioned problematic approach, Edgar Schein claims that the culture can be defined as (a) a pattern of basic assumptions, (b) invented, discovered, or developed by a given group, (c) as it learns to cope with its problems of external adaptation and internal integration, (d) that has worked well enough to be considered valid and, therefore (e) is to be taught to new members as the (f) correct way to perceive, think, and feel in relation to those problems.

Edger Schein also emphasises that there are visible and invisible levels of corporate culture (the culture iceberg analogy – the visible levels (surface manifestations) of the culture iceberg incorporate observable symbols, ceremonies, stories, slogans, behaviours, dress and physical settings. The invisible levels of the culture iceberg include underlying values, assumptions, beliefs, attitudes and feelings. Often, change strategies focus on the visible levels. (Schein, 1990, pp. 109-119)

One of the widespread perceptions of the essence of culture is that it is a way of thinking, acting and interacting. This definition, though too short and uncompleted, shows that culture has at least two aspects – cognitive and behavioural.

Having in mind all these understandings of culture in general security culture could be defined as a way of thinking and acting in regard of threats and dangers to the organizational interests. Therefore, business security culture could be defined briefly as a way of thinking and acting in regard of threats and dangers to the business organization's interests.

The concept of security culture is relatively new. It is often investigated in a simplistic manner focusing on the end-users and on the technical aspect of security (content approach). Security, however, is a management problem and as a result, the investigation of security culture should also have a management focus.

According to Igor Khripunov, security culture is a human factor based approach to improving security through more efficient human performance and interaction with systems, products, and the work environment. (Khripunov, 2008, p. 2)

Kai Roer points out that the security culture is the ideas, customs and social behaviours of a particular people or group that help them be free from threat and danger or the ideas, customs, and social behaviour of a particular people or society that allows them to be free from danger or threats. In this definition he incorporates/includes two other definitions – the definition on culture and the definition on security published in the Oxford dictionary. According to the Oxford dictionary, culture can be defined as: "Ideas, customs and social behaviour of a particular people or group." Security is "the state of being free from danger or threat." (Roer, 2015, pp. 12-13)

The same author slightly modified the above definition in his presentation "How Measuring Security Culture is Different from Counting Employees", delivered at the RSA Conference in 2017: "The ideas, customs and social behaviours that influence security." In this definition he has considered the fact that the security culture could have positive effects (e.g. when it is not underestimated) or negative (e.g. when it is underestimated) effects on the state of the organization.

Roer identifies three elements of the security culture – people, policies and technology (See Table 2). A constant interaction exists between them. Each of these elements directly impacts the other two. No matter where the change happens, the other two elements are changed too. Better understanding of their formation and their continued interaction makes easer building and maintaining security culture. (Roer, 2015, pp. 19-22)

Table 2. Elements of the Security Culture

Element	Essence
People	Hold competence/awareness; use technology and form and inform the policy
Policy	Written and unwritten laws, rules**,** regulations, ethics, moral codes that regulate ideas, customs and social behaviours
Technology	Any tool – made or not – used in a determined way (including tangible things like computers, cars, hammers and so on, but also models: mental models (patterns and schemas in our mind) as well as patterns, standards and models used as templates and starting points)

Source: Roer, 2015, pp. 19-22

According to the same author, security awareness is a key notion in the concept of security culture. It belongs to people – one of the elements of security culture.

The main difference between security awareness and security culture is that culture is more than just awareness. While the security culture is a combination of people, policy and technology, awareness is only about people, and only a subset of the people: it is knowledge only. (Roer, 2015, p. 23)

A lot of researches have been conducted on this topic (Dinev and Hu 2007, D'Arcy et al. 2009, Bulgurcu et al. 2010, Haeussinger and Kranz 2012). All of them have confirmed the importance of the awareness for the security of the organization. They found that the increase of awareness has a positive effect on the security behaviour performance and the whole level of security of the organization. (Haeussinger and Kranz, 2012, p. 2)

Awareness could mean several things. It could mean knowledge about security matters related to the organization and security measures, laws, rules, regulations etc., which regulates the behavior. It also could be accepted as a competence related to the use of security technologies.

In a broader sense, awareness could pertain to the perception of the internal and external environment as favorable or hostile to the organization. Such perceptions generally precipitate a certain behavior, specific actions and operations.

Awareness could be created, built and developed. This is one of the main goals of the security management of each organization. The role of top managers, in particular security managers, is to create right security awareness and ensure that this knowledge be applied in a certain situation.

There are different criteria on the basis of which business security culture is classified. The specific sector and activity, the utilized raw materials are just some of them. Some activities involve higher risks and require that stronger security measures should be taken and better security culture should be developed.

The nuclear security culture typical of the organizations working with nuclear and other radioactive materials (nuclear facilities, healthcare institutions and businesses) is a case in point. It is defined as the assemblage of characteristics, attitudes and behaviour of individuals, organizations and institutions which serves as a means to support and enhance nuclear security. (IAEA Nuclear Security Culture Series № 7, 2008, p. 2) The International Atomic Energy Agency (IAEA) has developed guidelines and provides assistance to help Member States establish a strong nuclear security culture. An effective nuclear security culture can result in a significant increase in the effectiveness of the security of radioactive material and associated facilities and transport.

The size of the business entity and organizational experience has also impact on the security culture. The absence of clearly defined security rules and procedures, as well as training programs in terms of security is typical for the small private businesses dealing with not too risky activity.

According to the scale of the development of its elements – rules**,** regulations, ethics, moral codes, technologies, skilled and security aware staff and their

effective interaction security culture could be categorized as developed and undeveloped one. At this basis it also could be classified as strong or weak.

The topic of measuring security culture is essential in terms of above categorization. As there are not units of its measuring this assessment should be done by an indirect manner. Business security culture is a foundation of the business security which also could not be measured but there are other objective indicators which enable the level of security to be defined as low or high. E.g. such indicators could be the frequency of malicious acts to the organization, their prevention or their success, as well the scale of the damages and losses after their happening.

Having in mind this it could be claimed that the strong security culture, in ceteris paribus, guarantees higher level of security whereas the weak security culture means low level of security related to threats and incidents causing negative consequences for the interests of the business entity.

Building a Business Security Culture

Building and maintaining business security culture is a management activity. Edger Schein highlights that the only thing of real importance that leaders do is to create and manage culture; that the unique talent of leaders is their ability to understand and work with culture; and that it is an ultimate act of leadership to destroy culture when it is viewed as dysfunctional (Schein, 2004, p.11).

Igor Khripunov points out that security culture is a vehicle to improve the human factor through a set of managerial, organizational and other arrangements that include not only the technical proficiency of the people entrusted with security but also their willingness and motivation to follow established procedures, comply with regulations, and take the initiative when unforeseen circumstances arise. (Khripunov, 2008, p. 2)

Building security culture and especially its maintaining is a constant and continues process. Chris Romeo claims that an organization's security culture requires care and feeding. It does not grow in a positive way organically. A sustainable security culture is bigger than just a single event. When a security culture is sustainable, it transforms security from a one-time event into a lifecycle that generates security returns forever.

Building security culture is a process, which includes the basic management functions: planning (setting organizations' goals related to building a business security culture and deciding how best to achieve them), organizing (determining how to group the activities and resources in the best way), leading (motivating members of the organization to work in the best interest of the organization in the context of the set goals) and controlling (monitoring and correcting ongoing activities to facilitate goal attainment).

One of the main aspects of management activity is taking of responsibility. The responsibilities apply to the setting and achieving specific goals. The managers are responsible for building and maintaining security culture in the organization. They assume the responsibility. The main challenge faced by them is to take timely decisions that are relevant to the needs and specificities of the organization. It depends mainly on their personal characteristics, competences and their attitude to the security matters in general.

Resources, which are allocated for building and maintaining business security culture, depend on objective and subjective circumstances. An objective reason is the financial condition of the organization and its activities. The better its economic condition, the more resources it will be able to allocate for security purposes. A subjective factor, as mentioned above, is managers' attitude to security issues. Prioritizing these issues will mean allocating sufficient resources to security and developing stable security culture in the organization.

Having in mind the three elements of security culture – policy, people, technology, already mentioned above in the current publication, the management activity and management functions in particular must be focused on their development and maintenance.

Policy – It is a building block of business security culture, encompassing internal organizational norms, procedures and ethic codes that determine staff's attitudes and behavior. Its main goal is to guarantee the needed level of security for normal functioning of business entity.

The development of certain policy is security managers' responsibility. Setting certain rules, they take into account the characteristics of the organization (e.g. mission, objectives, activity and personnel) and existing risks in the internal and external environment.

The policy affects all aspects of business security: information security, physical security, personnel security.

Information security means protection of information resources. These resources are created, processed and stored in the organization. Sometimes the organization uses information created by other organizations. The information security policy gives the rules that have to be observed by the staff to ensure the protection of an important for business interests' information.

Physical security is related to protection of organization's assets – tangible (land, buildings, all kind of equipment, money etc.) and intangible (trademarks, patents, image etc.). It also includes protection of the staff and clients from different kind of risks and threats. The physical security policy aims establishment of a less risky environment for these assets.

The personnel security policy implements norms and procedures, which has to provide loyal, trustworthy staff in terms of security and protection of the

organization's secrets. In a broad sense motivation policy could be an aspect of this policy.

People – The employees must be familiar with the security policy of the organization and informed about the changes of this policy. For this purpose, they periodically participate in different trainings. During these courses the staff becomes acquainted with the norms and the security requirements. The most important role of these trainings is development of security awareness – knowledge about security matters, attitude to security matters and behavior, which does not underestimate security.

Many authors give practical advices to develop security culture, most of them are directly related to the people. Chris Romeo presents a few steps, which support building of security culture from the top to the bottom in an organization. He points out that the building of security culture has to begin with engagement of all the staff in the process. **M**any organizations have the opinion that the security department is responsible for security. Sustainable security culture requires that everyone in the organization is all in. Everyone must feel like a security person. This is security culture for everyone. Security belongs to everyone, from the executive staff to the lobby ambassadors. Everyone owns a piece of the company's security solution and security culture.

The next step is development of security awareness through teaching the entire team the basic lessons about security. Romero also recommends **reward and recognition for** those people that do the right thing for security. E.g. when someone goes through the mandatory security awareness program and completes it successfully to be stimulated with some kind of reward.

A final step is to provide an opportunity to earn an advanced degree in security. Many universities offer a master's degree programmes in security. The organization can sponsor students, which will be a positive message to the staff.

Building a security community is another important element. Security community is the backbone of sustainable security culture. Community provides the connections between people across the organization. Security community assists in bringing everyone together against the common problem, and eliminates an "us versus them" mentality. (Romero, 2016)

Technology – It means presence of technologies used to ensure business security and their proper exploitation by the staff. The availability of advanced security technologies depends on: a) the specifics of the business organization's activity, b) the presence of threats to it, c) business organization's financial status, and d) the attitude of the managers towards the security issue.

Conclusion

At the end of this paper, it should be emphasized yet again that business security is based on business security culture. It has two aspects – cognitive and behavioural. Above all it is a way of knowing and understanding of the things and processes that take place in the internal and external environment and then a reaction regarding to these things.

Building and maintaining security culture is a challenge that managers invariably face. It is constant process which includes the development of norms, procedures and ethic codes and their periodic update, as well. This process needs resources.

Security awareness is an essential part of the concept of business security culture. It is developed and maintained during training and other courses, organized inside or outside of the business entity. In essence, security awareness means that employees informed of security matters (they are aware of the importance of security), observe the existing security rules (they know and respect the norms and rules) and face and overcome different security-related challenges by means of the available technologies (they are prepared to use all kind of technologies).

Future research and publications in this field could be focused on the methods and techniques for developing security culture in business organizations with specific activity form different economic sectors (e.g. Nuclear Sector or other sectors, using nuclear materials [3]). Building security awareness, as well as developing of policies concerning specific types of security on organizational level (physical, personnel, information etc.) also are very interesting topics for further study. The measuring and assessing the security culture is another matter that deserves attention.

Notes:

[1] All organizations and all business organizations in particular are community of people, who works together and striving to achieve certain goals. They are social systems and have their interests, which try to protect effectively in the conflicts.

[2] In his D.Sc. thesis, defended at the National and Regional Security Department at UNWE in 2016, Kiril Stoychev presents the Integrated System for Security Management in Organization. He climes that this system includes different levels of security and protection, such as: Level 1 – Risk Assessment and Internal Security; Level 2 – Risk Assessment, Internal Security and External Security; Level 3 – Risk Assessment, Internal Security, External Security, Quality Assurance and Safety; Level 4- Risk Assessment, Internal Security, External Security, Quality Assurance and Safety, Information Security, Human

Resources and Financial Security; Level 5 – Risk Assessment, Internal Security, External Security, Quality Assurance and Safety, Information Security, Human Resource, Financial Security Environmental Security and Social Corporate Responsibility; Level 6 – Risk Assessment, Internal Security, External Security, Quality Assurance , Safety, Information Security, Human Resource, Financial Security Environmental Security, Social Corporate Responsibility and Business Continuity Management. (Stoichev, 2016, p. 10)

[3] Prof. Dr. Dimitar Dimitrov (chief scientific investigator) – head of Department National and Regional Security at the UNWE, Assoc. Prof. Dr. Georgi Penchev and Dr. Atanas Dimitrov, both members of the academic team of Department National and Regional Security at the UNWE, participated in the Coordinated Research Project "J02007" Development of Nuclear Security Culture Enhancement Solutions (2016-2018), funded by IAEA. Their study is dedicated to nuclear security culture in medical facilities in Bulgaria. This participation is within the Master's Degree Program in Nuclear Security offered by the Department of National and Regional Security at the UNWE, Sofia, Bulgaria in cooperation with the IAEA and other government and scientific institutions.

References:

Димитров, К. (2012), Фирмена култура, ИК-УНСС София
(Dimitrov, K. 2012, Firmena kultura, IK-UNSS, Sofia)
Паунов, М. (2015), Организационна култура, ИК-УНСС, София
(Paunov, M. 2015, Organizatsionna kultura, IK-UNSS, Sofia)
Слатински, Н. (2011), Сигурността: същност, смисъл и съдържание, Военно издателство София.
(Slatinski, N. 2011, Sigurnostta: sashnost, smisal i sadarzhanie, Voenno izdatelstvo, Sofia)
Стефанов, Г. (2008), Теория на международната сигурност, Сиела София
(Stefanov, G. 2008, Teoria na mezhdunarodnata sigurnost, Ciela, Sofia)
Стойчев, К. (2016), Структурно-функционален подход за управление на сигурността и защитата на критичната инфраструктура, автореферат за придобиване на научна степен "доктор на науките", София.
(Stoychev, K. 2016, Strukturno-funktsionalen podhod za upravlenie na sigurnostta i zashtitata na kritichnata infrastruktura, avtoreferat za pridobivane na nauchna stepen "doctor na naukite", Sofia)
Тагарев, Н. (2011), Предвиждане на уникалните заплахи за информационната сигурност, Сборник с доклади от Международна конференция: Прилагане на информационните и комуникационни технологии в науката и образованието (ICAICTEE-2011), София.

(Tagarev, N. 2011, Predvizhdane na unikalnite zaplahi za informatsionnata sigurnost, Sbornik s dokladi ot Mezhdunarodna konferentsia: Prilagane na informatsionnite i komunikatsionni tehnologii v naukata i obrazovanieto)
Alvesson, M. (2013), Understanding Organizational Culture, Los Angeles: SAGE Publishing
B Corporations, Benefit Corporations and Social Purpose Corporations: Launching a New Era of Impact-Driven Companies [Online], Network for Business Innovation and Sustainability (NBIS), Available at http://nbis.org/wp-content/uploads/2012/10/ImpactDrivenCompanies_NBIS_Whitepaper_Oct2012.pdf , (Accessed: 19 October 2017)
Buralton, R. (2001), Principles of Process Management (Online), Available at: http://www.informit.com/articles/article.aspx?p=131055, (Accessed: 26 July 2018)
Bremer, M. (2012), Organizational Culture Change, Zwolle, Netherlands: Kikker Groep
Cameron, K. S. (2006), Diagnosing and Changing Organizational Culture: Based on the Competing Values Framework, San Francisco, John Wiley & Sons
Dimitrov, K., M. Geshkov. (2018), "Dominating Attributes of Professed Firm Culture of Holding Companies – Members of the Bulgarian Industrial Capital Association", in Economic Alternatives, Issue 3, pp. 384-418
Haeussinger Felix J. and Kranz Johann J. (2013),"Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior" paper presented at the Thirty Fourth International Conference on Information Systems [Online], Milan, Italy, Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.669.8230&rep=rep1&type=pdf, (Accessed: 15 September 2018)
Human Resource, BusinessDictionary (Online), Available at: http://www.businessdictionary.com/definition/human-resource.html, (Accessed October 13, 2017)
Khripunov, I. (2008), "Russia's Security Culture and WMD Proliferation", presented at: Tomorrow's Proliferation Pathways: Weak States, Rogues, and Non-States, July 17-18, 2008, Belfast. (Accessed: 15 April 2015)
Kraaijenbrink, J. and Groen, A. (2012), "Towards a Functional Resource-Based Theory of the Firm" paper presented at the SMS 28th Annual International Conference (Online), Cologne. Available at: http://kraaijenbrink.com/wp-content/uploads/2012/06/Towards-a-functional-RBV-Kraaijenbrink-Groen-12-10-2008.pdf , (Accessed 30 October 2017)
Martin, J. (2004), Organizational Culture, Research Paper №1847, Stanford Graduate School of Business
Nuclear Security Culture, Implementing Guide, IAEA Nuclear Security Series №7, Vienna, 2008

O'Donnell O. and Boyle R. (2008), Understanding and Managing Organizational Culture [Online], Available at: https://www.ipa.ie/_fileUpload/Documents/CPMR_DP_40_Understanding_Managing_Org_Culture.pdf , (Accessed: 30 July 2018)
Ouchi W. G. and Wilkins A. (2003), "Organizational Culture", in Annual Review of Sociology 11(1), pp. 457-483
Roer, K. (2015), Build a Security Culture (Online), Available at: https://news.asis.io/sites/default/files/Build%20a%20Secuirty%20Culture%20%28Fundamentals%20Series%29%20by%20Kai%20Roer.pdf, (Accessed: 20 July 2018)
Romero, C. (2016), Nurture the Ninjas within. 6 Ways to Develop a Security Culture from Top to Bottom, Available at: https://techbeacon.com/6-ways-develop-security-culture-top-bottom , (Accessed: 15 August 2018)
Schein, E. H. (2004), Organizational Culture and Leadership, Jossey-Bass, San Francisco.
Schein, E. H. (1990), "Organizational Culture", in American Psychologist, 45, pp. 109-119

DEVELOPING AND MAINTAINING BUSINESS SECURITY CULTURE

Abstract

Security is an extremely important issue. All social systems need security to function and to achieve their goals. Some of these are business organizations. Business security culture is a foundation of business security. Building and maintaining security culture has a managerial aspect and is related to management. The goal of the current paper is to draw attention to this topic. It aims to shed light on the main aspects of the subject. The article makes an attempt to perform three main tasks, namely the analysis of: 1) the business security concept; 2) the concept of business culture; 3) the development and maintenance of business security culture.

Key words: business security, corporate security, **s**ecurity culture, business security culture.

JEL: M14, L20