Where is the Place of Corporate Security/Safety in the Organizational Structure of an Organization – An Approach

ZORAN R. PENDIĆ, UETS Development Centre, Belgrade
RAJKO Z. PENDIĆ, Eurosolutions, Belgrade
BOJANA B. JAKOVLJEVIĆ, Telekom Serbia, Belgrade
LJILJANA B. VUJOTIĆ, Clinical Centre of Serbija, Belgrade
LAZAR T. GAJIĆ, UETS Development Centre, Belgrade

Original scientific paper
UDC: 005.922.1
DOI: 10.5937/tehnika1905741P

The terms „Safety" and „Security" are too often used as synonyms in many languages. But, safety and security doesn't mean the same thing. It is very important for the safety / security of business processes and the protection of business interests of any organization that the management of that organization understands the difference between these two terms. Also, the management of the organization should well define the tasks and place(s) of security / safety system in the organizational structure. The security / safety system of an organization should be considered as the system deeply connected to all parts of business system.

The importance of the security / safety system in improving the overall business system of an organization is increasingly understood in Serbian organizations, as a well-established security / safety system significantly reduces the risks of potential business losses of any kind. To emphasize, if the top management of an organization has a dilemma whether or not to establish a security / safety system, we can recommend: Establish, it pays off!

Key words: *safety, security, business system, organizational structure*

1. INTRODUCTION

The terms „Safety„ and „Security‟ are too often used as synonyms in many languages.

In our (Serbian) technical papers *safety* is the most frequent word for both terms, whereas in Croatia it is – *security*.

In Norwegian the word 'sikkerhet' translates both security and safety. In German that word is Sicherheit, in Spanish – seguridad, in French – securite, and in Italian – sicurezza [1-10].

But, safety and security doesn't mean the same thing. It is very important for the safety / security of business processes and the protection of business interests of any organization that the management of that organization understands the difference between these two terms.

„Safety focuses on the potential result of an occurrence defined as a risk. Meaning something is identified as a Safety problem if there is an unacceptable risk of damage to people, property or the environment. A Security problem is independent of the result of the action. A Security problem refers to illegal or unwanted penetration, interference with proper operation or inappropriate access to confidential information regardless of motivation (intentional or unintentional) or consequence (result)‟ [1].

In ref. [2], the subtle difference between these two terms is explained in a comprehensible way: „Security can be seen as an umbrella which keeps us out of the rain (Figure1). Our safety is reflected in the fact that we are dry and not cold under the umbrella. Security is protection which makes sure our safety is constant. If it is possible to predict variables risky to our safety, possible risks could be avoided or reduced to acceptable level by carrying out certain preventive measures. For example, we could keep comfortable temperature in our flats by air-conditioning settings. Locks secure entry doors. However, our property surroundings cannot be controlled so easily. Weather forecast can warn against rain, but safety still requires our involvement. Hence, Awareness or perception of a

Author's address: Zoran Pendić, UETS Development Centre, Belgrade, Kneza Miloša 7a/I

e-mail: razvojni.centar@sits.rs

Paper received: 06.09.2019.

Paper accepted: 20.09.2019.

situation or fact+Preparation=Safety‟. Or [9], mathematically speaking: Safety=Security+Perceived value (the sense of being safe).

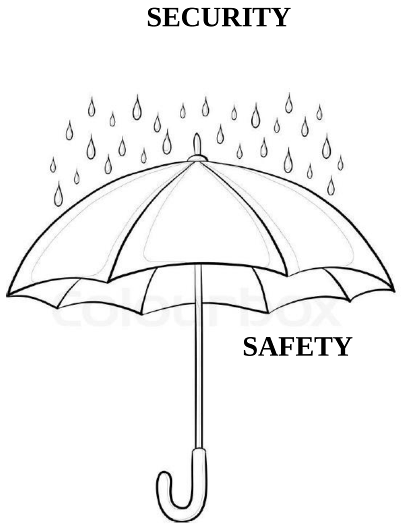
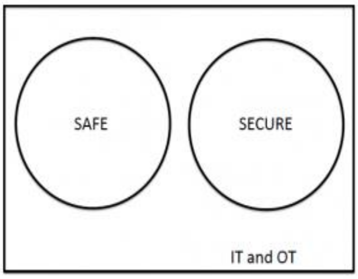


Figure 1 - Security and safety [2, 12]

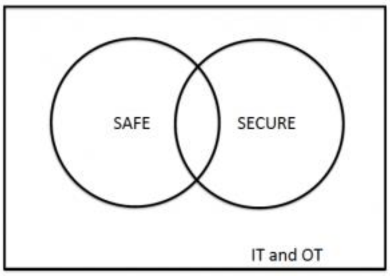
Here is how TÜV NORD [11] explain the difference between security and safety from the aspect of security and safety in industry: *Safety* means avoidance of accidents and *security* means crime prevention. Take the example of emergency exit: both aspects are there, safety and security. In terms of *safety*, you have to be able to leave the building at any time, and emergency doors should always be open. As for security - with focus on building protection - those doors should not be there at all, so no one can enter the building. Aims and benefits of security and safety are sometimes contradictory, which is exactly what makes this subject so intriguing. To protect people and environment, traditional safety measures are applied to potentially dangerous machinery. However, as regards security, you are not protecting people from machinery - but vice versa: you have to protect machines from people against malfunctioning, grinding to a halt or cancelling safety precautions.

Safety and security play an important role in Industry 4.0. What's the difference between security and safety concepts in this industry? The answer can be found in the lit. [11,13]. Authors of this paper believe that water supply systems, due to their complexity and increasing automation and digitization, have important characteristics of the industry 4.0. According to [13], in the context of industrial automation and control systems, safety systems are special control systems whose function is to detect a hazardous condition and take action (typically shut down the process) to prevent a hazard. They are typically one of many layers of defense in an overall protection scheme for the facility. On the other hand, security of control systems refers to the ability of control systems to provide adequate assurances that unauthorized persons and systems are neither allowed to modify software and its data nor permitted access to system functions, making sure these are not denied to authorized personnel and systems.

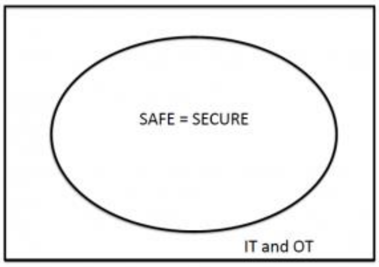
We will point out another good reference dedicated to Industry 4.0. Ref. [3] indicated that „Increasing digitization has led to convergence between IT (Information Technology) used in offices and mobile devices, and OT (Operational Technology) that controls devices used in critical infrastructure and industrial control systems. The IoT (Internet of Things) is also rapidly growing, with around 10 billion devices today. These trends raise concerns about the interaction between safety and security… From a regulatory and standards point of view, the following Venn diagram summarises the current situation:



However, practitioners recognize that there is not a clear separation (indeed it would be undesireable if there was), so the following is a better diagram of the current situation:



There is a question about how large the intersection should be. There appears to be general agreement that the following diagram is wrong:



The debate about the interaction between safety and security will continue.‟

Also we need to point out here an extremely important industry where the security / safety system plays a particularly important role. This is Healthcare industry [14-31].

In ref. [14] it is indicated that: "By 2050, the world will be home to 10 billion people, and two in five of these people will be aged 60 or over, including 434 million over 80 years old. This combination of population growth and demographic changes will seriously accelerate the challenges we face for the delivery of health and healthcare, with global healthcare spend projected to reach 13% of GDP in OECD countries by 2050.‟

Ref. [14] also point out that: „The rapid pace of advances in science and technology in the Fourth Industrial Revolution has important implications for health and medicine. Advances in fields such as genetics, genetic engineering, precision medicine, data science, and more are giving rise to new diagnostic and therapeutic modalities which offer the possibility of curing disease, reducing suffering, lengthening lives, and more.‟

Ref. [14] specifically highlights the vulne-rability of hospitals and health systems to cyberattacks, which could be dangerous for both patients and staff. Moreover, such attacks to broader infrastructure, for example to electric grid, could stop hospitals/healthcare organizations from functioning. Any physical facilities, as MRI, PET-CT etc. conected to elecrtical grid is potentially at risk from being taken over and exploited by hackers. Particular attention should be paid to cyber attacks on small healthcare organizations [22].

Security/safety system in any healthcare organization should be designed and implement carefully. It should be based on an organization's security/safety culture and spread throughout all parts of the organization. Because of the extreme importance of the Healthcare industry, the authors intend to dedicate special paper to implementation of the security / safety systems in this industry.

Our introductory notes here are fully in keeping with the Merriam-Webster definition of safety and security [13, 32, 33], where the primary definition of safety „the condition of being free from harm or risk‟ is basically the same as the primary definition of *security:* „the quality or state of being free from danger‟. However, there is one more definition of security [13], which is "measures taken to guard against espionage or sabotage, crime, attack or escape", and that is generally the definition used when referring to industrial security.

Definitions of safety and security referenced in [8] are also interesting: Safety is protection against random incidents. Random incidents are unwanted incidents that happen as a result of one or more coincidences; Security is protection against intended incidents. Wanted incidents happen due to a result of deliberate and planned act.

2. TASKS AND FUNCTIONS OF CORPORATE SECURITY/SAFETY

Corporate security/safety dates back several centuries. However, the roots of contemporary corporate security/safety in Western Europe and USA go back to the 30s of the 20th century, when certain laws in this area began to be adopted. In countries of the West Balkans, dealing in more detail with this important area started towards the end of the last century. Legal solutions that partially cover corporate security/safety in Serbia are given in Ref. [34].

This paper will not cover in much detail tasks and functions of contemporary corporate security/safety. Because of the immense importance of this field for overall business activities of organizations of any type, a more detailed study of tasks and functions of corporate security/safety will be the subject of further series of papers prepared by contributors of the Development Centre of the Union of Engineers and Technicians of Serbia (DC UETS). Also, DC UETS will put together team of experts in this area to prepare one-day and several days training seminars for employees of various types of organizations, with special emphasis on training of water supply companies. References 1-66 make a good starting foundation for the study of corporate security/safety.

A „defensive‟ approach to corporate securety/-safety dominated before, focused on protection and prevention of losses. Many people today still identify corporate security/security with physical protection within the organization.

However, security/safety of performing business processes and protection of business interests of organizations present the most vital segment of contemporary corporate security/safety. The processes of corporate security/safety are ranked among key processes of the organization's business system, and contemporary corporate security/safety has become a strategic function in organization.

Let us set out some basic tasks and functions of corporate security/safety:

- physical and technical security/safety (organization's infrastructure);
- industrial security/safety (factory plants; control systems);
- healthcare security/safety (patients, staff, healthcare organization’s infrastructure);

- personal security/safety (work environment, surroundings of the workplace, safety and health at work);
- administrative security/safety (documents, policies);
- information security/safety;
- security/safety of intellectual property and business partner relationships;
- fire protection (people, infrastructure);
- protection from criminal activities;
- security/safety of contracting processes and concluded contracts;
- security/safety of managers;
- crisis management;
- business events security/safety;
- programs of continuing education of employees in the field of corporate security / safety in accordance with the principles of the learning organization...

It should be noted that within corporate security/-safety, due to exponentially growing cyber-attacks on information and control systems functioning within organization, special attention is given to IT security/safety. Available data show that human factor causes 70% of business information loss. Some of standard procedures for protection of computer network include: restricted Internet access for personnel, scanning e-mails for viruses and setting up company intranet.

Due to the great importance of information security/safety, it is important that any organization of any type, regardless of its size, should harmonize its business system with regard to information security/safety with the requirements of international standards ISO/IEC 27001:2013 (ISO/IEC 27001:-2013/Cor 1:2014, ISO/IEC 27001:2013/Cor 2:2015), ISO/IEC 27002:2013 (ISO/IEC 27002:2013/Cor 1:2014, ISO/IEC 27002:2013/Cor 2:2015), and the entire business system with the requirements of ISO 9001:2015 [66]. This recommendation applies fully to water supply companies as well.

We should point out that special attention has been paid lately to cyber terrorism, i.e. terrorist and vandal hacking attacks on SCADA (Supervisory Control And Data Acquisition) systems for remote supervision and control in water supply systems. In the first half of 2016, for example, hackers attacked an unnamed major water supply system in an unknown location in the USA- the level of chemicals used in water treatment was changed.

According to WEB page of ISO, International standard ISO/IEC 27001:2013 [64], adopted in Serbia as SRPS ISO/IEC 27001:2014, specifies requirements for setting up, application, functioning, monitoring, reassessment, maintenance and improvement of documented information security management system within the context of total business risks in an organization. International standard ISO/IEC 27002:-2013 [65] (SRPS ISO/IEC 27002:2015) provides guidelines for organizational information security standards and information security management practices including choice, implementation and management of controls, taking into account considerations od organization’s surroundings dangerous to information safety.

The basic International management standard ISO 9001:2015 (SRPS ISO 9001:2015) gives free rein to „risk-based thinking“ in organization’s business system. It is its main feature.

To conclude this paragraph with the fact that, regarding corporate security/safety, most Serbian organizations share these features:

- inadequate awareness of need to set up suitable security/safety mechanisms in organization;
- corporate security/safety is not seen as organization’s strategic issue;
- pay much more attention to external threats to the organization’s security/safety, though employees jeopardize security/safety procedures in more than 70% of cases, as worldwide experience suggest.

3. THE PLACE OF CORPORATE SECURITY/ SAFETY IN ORGANIZATIONAL STRUCTURE

Many management experts adopt a systems approach to business processes management, whereby the entire environment is taken into account rather than mere effect of individual jobs or operations. Organization (company) is viewed as a system, with parts i.e. subsystems united for accomplishing common goals. When making decisions, a successful manager has to study relationship between subsystems, and identify basic and auxiliary processes in the company that affect creating added value. This integrated approach helps avoid situations where solving a problem in one area becomes a problem in another one. The system theory presumes that no action can be taken in isolation, but each decision spreads across the entire system.

The organization of any type should apply a systems approach to business processes management, which implies: identifying, understanding and managing interconnected processes as a system that contributes to efficiency and effectiveness of the organization in achieving its goals. The main task of the organization's management is to identify and then manage main and auxiliary processes within the organization's global task, applying modern IT infrastructure in achieving it.

For an organization to be able to manage a business process-based system, it is necessary to firstly define a network (map) of its basic processes. The criterion for defining basic processes are their connection and impact on meeting the organization's strategic goals. For a proper selection of basic business processes it is necessary to define the total flow of business, from the initial request of the user/buyer/investor to the delivery of product/service.

Therefore, work in the organization of any type is carried out through a network of processes, whereby the structure of process network depends on the complexity of company programs/projects. The network is comprised of processes linked to performing all functions of the organization (planning; research; design; technologies; production functions: production preparation, production, providing services; quality control; training; human resources; marketing; ecology; procurement; sales; finance; (JIT) maintenance; communications with business partners; security/safety/functional safety, etc.).

In organizations where the structure is based on work processes management (horizontal structure), responsibilities shift from individuals to teams.

Key (major) processes:

- spread across functional borders of the organization;
- the outcomes of these processes are strategically important for the organization's success;
- have a decisive influence on meeting requirements/expectations of the user/buyer/investor.

Business processes in any type of organization generally fall into three groups:

- key processes of the business system,
- support processes,
- processes of management.

Clearly not all business processes are equally important, even though the main goal of business process management is to systematically improve all processes from the organization's network of business processes. Special attention should be paid to the continuous improvement of the macro process, especially those macro processes that are necessary for achieving the strategic goals of the organization. Such processes are the driving force of an organization and are crucial for its survival. That group of strategic macro processes forms a set of the so-called key (main) processes.

Depending on complexity and nature of programms/projects being performed within the organization, it is usually possible to distinguish between ten and twenty key processes. A process can be classified into a set of key processes if: (i) it affects the organization's strategic objectives, (ii) its output is linked to investor/buyer/user (patient), (iii) it is necessary in relation to customer user/buyer satisfaction. Processes that supervise other processes are not included into key processes; also processes which are not vital for survival of the organization.

Support and processes of management, albeit not directly affecting investor/buyer/user satisfaction, do fall among key processes if they have strategic significance for achieving business policy of the organization (e.g. strategic planning, IT system, unique system of marking all business elements, legal services, financial services, security/safety of operations, risk management; also total quality management, business policy, reviews of certain jobs/operations, personnel management, etc.). For a proper selection of key business processes one has to define complete business flow, from the initial request of the investor/buyer/user to delivery of product/service.

In contemporary functional-matrix model of organization structure [35], experts of different profiles can be combined for a one-off job/project, and then move on to others. That way their knowledge, expertise and qualifications are efficiently used. Such an organizational structure is suitable for organizations that work in a dynamic environment and realize complex services / products. Here, teamwork (matrix part of the structure) is applied to those jobs and projects where a functional organization is unsuitable.

Organizational units of the organization that provide services to business and projects carried out within the organization, such as marketing, sales, procurement, finance, development, quality ..., are functionally organized. Production of products/services is functionally organized. As a function, the production of products/services can, in certain types of organizations, provide services to certain one-off jobs/projects that are performed in the organization. Problems likely to arise with functional matrix model of organization’s structure are those concerned with responsibility, authorization and coordination of work while performing simultaneous jobs/projects. This is solved through certain defined procedures of the organization's business system. Possible solutions to conflict situations are proposed at the top level of organization's management.

From the previous consideration in this section of the paper it is clear that processes performed within the security/safety function belong with support processes to the organization's business system. Corporate security/safety in the organization plays an important part in achieving the set strategic goals of the organization.

Depending on the organization's size and activities, securety/safety activities are done by one ore more teams of experts from different company units, with clearly set resposibilities and authorizations. The coordination of the work of the teams is carried out, as a rule, by a manager from the top management structure, with the full cooperation of the top management.

Obviously corporate security/safety in Serbia is gaining momentum as it improves the entire company business system, significantly reducing losses.

A detailed description of the work of the members of corporate security/safety teams will be the subject of forthcoming papers. Necessary knowledge, skills sets, capabilities and personal traits expected from team members will also be dealt with.

4. CONCLUSION

There is no denying that corporate security/safety is sine qua non in today's business environment in various types of organizations. It is also clear that introducing security/safety into business systems is a demanding and long-term chore. In some companies it can take several years. Obviously, favorable results of introducing this function are not visible at once, which often discourages top managerial teams and puts them into dilemma if the whole shebang pays off at all. Let us remove the dilemma: IT definitely DOES PAY OFF.

We should point out that the influence of teams performing security/safety activities is proportionate to their capability to convince individuals and other teams within company to cooperate. Hence, they have to establish with them long-lasting, open and fruitful dialogue. In other words, security/safety teams must not even try to count on lack of knowledge of others in their favor.

It is indisputable that corporate security / security, in today's business environment in which organizations of different type are working, is necessary. It is also clear that the introduction of a security / security function into an organization's business system is a required and long-term job, which may take several years for some organizations. It is evident that the positive results of introducing this function can not be seen immediately, which can often discourage the top management of the organization and introduce the dilemma of whether the entire business is worth it at all. To resolve the dilemma: SAFE WILL BE DISCLAIMED.

It should be noted that the impact of teams that implement activities within the security / safety function is proportionate to their ability to convince individuals and other teams throughout the organization to cooperate, which means that they have to establish a lasting, open and fruitful dialogue with them. In other words, safety / security teams should not even try to play the lack of knowledge of others for their own benefit.

Also, when setting up security/safety function within company business system, one should not look for Rolls Royce solutions as absolute security is not possible, and such solutions are not financially justifiable.

What matters when setting up this function is establishing good relationships within company and good relationships between company and its interested parties.

The outcome of activities pertaining to this function must be visible across the whole of company and help come up with right strategic decisions within the business system.

Also, in establishing the security / safety function within the organization's business system, Rols-Roice solutions should not be sought, because absolute security is not possible, and economically such solutions are not justified.It is important that in establishing this function, in addition to good relations within the organization, good relations between the organization and its stakeholders are also good.

The results of the activities that take place within this function must be visible throughout the organization and contribute to making correct strategic decisions within the business system. At the end, the importance of the organization's security culture existence should be emphasized. Security culture does not originate on its own. It needs to be invested in it in the long run. When an organization's security culture becomes sustainable, it transforms security from a one-time event into a lifecycle that provides security on an ongoing basis.

REFERENCES

[1] The rocky relationship between safety and security, [Internet], https://library.e.abb.com/public/3e234b767729aaa0c1257aa60064b129/3BUS095673_en_Whitepaper_-_The__Rocky_Relationship_between_Safety_and_Security.pdf

[2] Coursen S, *Safety vs. Security: Understanding the Difference May Soon Save Lives*, August 31, 2014, [Internet], https://www.linkedin.com/pulse/2014-0831152519-11537006-understanding-the-difference-may-soon-save-lives-safety-vs-security/

[3] Hankin C, The interaction between safety and security, Imperial College, Institute for Security Science & Technology, London, [Internet], https://wwwf.imperial.ac.uk/blog/security-institute/-2017/01/03/the-relationship-between-safety-and-security/

[4] Schwarz Carigiet D. What is the difference between word safety and security?, [Internet], .https://-www.quora.com/What-is-the-difference-between-safety-and-security

[5] Jore S. H, The Conceptual and Scientific Demarcation of Security in Contrast to Safety, European Journal for Security Research, Vol. 4, Issue 1, pp 157–174, April 2019, [Internet], https://link.springer.com/article/10.1007/s41125-017-0021-9

[6] Đukić S. Osnove i sistem bezbednosti u strategiji nacionalne bezbednosti, *VOJNO DELO*, str. 100-121, 7/2017, [Internet], http://www.odbrana.-mod.gov.rs/odbrana-stari/vojni_casopisi/arhiva/-VD_2017-7/69-2017-7-09-Djukic.pdf

[7] Komarčević M, *Uvod u bezbednost*, Priručnik (Priređivač: M. Komarčević), Visoka strukovna škola za preduzetništvo, Beograd, 124 str, 2017, [Internet], http://vssp.edu.rs/wp-content/uploads/-2019/03/Priru%C4%8Dnik-Uvod-u-bezbednost.pdf

[8] Albrechtsen E. Security vs safety, Norwegian University of Science and Technology, August 2003, 8 p., [Internet], http://www.iot.ntnu.no/users-/albrecht/rapporter/notat%20safety%20v%20security.pdf

[9] Difference between safety & security, Monday, June 17, 2019, [Internet], https://www.securitas.in-/articles-and-information/article---difference-between-safety--security/

[10]Difference Between Safety and Security, [Internet], http://www.differencebetween.net/language/words-language/difference-between-safety-and-security/

[11]Springer M. What's the difference between safety and security?, TÜV NORD GROUP, [Internet], https://www.tuev-nord.de/explore/en/explains/whats-the-difference-between-safety-and-security/

[12]Khan Z. What is the difference between safety and security?, Dec 14, 2016 [Internet], https://www.-quora.com/What-is-the-difference-between-safety-and-security

[13]Byres E., Cusimano J. Safety and Security: Two Sides of the Same Coin, [Internet], http://www.-controlglobal.com/articles/2010/safetysecurity1004/

[14]Health and Healthcare in the Fourth Industrial Revolution - Global Future Council on the Future of Health and Healthcare 2016-2018, World Economic Forum, Switzerland, Insight Report, 45 p., April 2019, [Internet], http://www3.weforum.org-/docs/WEF__Shaping_the_Future_of_Health_Council_Report.pdf

[15] Kohn L. T, Corrigan JM, and Donaldson MS, *Editors. To Err Is Human - Building a Safer Health System*, Institute of medicine, National academy press, Washington, D.C., 312 p., 2015.

[16] *Security trends in the healthcare industry*, IBM Security, IBM X-Force Research, Somers, NY 10589, 21 p., February 2017.

[17]Securing the healthcare enterprise - Taking action to strengthen cybersecurity in the healthcare industry, IBM Security, Somers, NY 10589, Thought Leadership White Paper, 16 p., March 2015.

[18] *National Safety and Quality Health Service Standards - Guide for Hospitals*, Australian Commission on Safety and Quality in Health Care, Sydney, 342 p., 2017.

[19] Security and safety at hospital, [Internet], https:-//www.betterhealth.vic.gov.au/health/servicesandsupport/security-and-safety-at-hospital

[20] Jahn Kassim PN, Abdul Manaf NH. Integrating patient safety and risk management: The role of law and healthcare organisations, *Journal of Global Business and Social Entrepreneurship*, Vol. 1, No. 2, pp. 115-125, 2017.

[21]Joseph A et al, *Designing for Patient Safety: Developing Methods to Integrate Patient Safety Concerns in the Design Process*, The Center for Health Design, Supported by the Agency for Healthcare Research and Quality (AHRQ), USA, 125 p, 2012.

[22] Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations, 29 p., 2018, [Internet], https://healthsectorcouncil.org/wp-content/uploads/2018/12/tech-vol1-508.pdf

[23] Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations, 108 p., 2018, [Internet], https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol2-508.pdf

[24]Abouelmehdi K et al. Big healthcare data: preserving security and privacy, *Journal of Big Data 5,* Article number: 1, 18 p., 2018, [Internet], https://-journalofbigdata.springeropen.com/articles/10.1186/s40537-017-0110-7

[25]*Isolation best practices for healthcare organizations - A Menlo Security Best Practices Guide*, Menlo Security, Palo Alto, CA, 10 p., 2018, https:-//www.menlosecurity.com/hubfs/pdfs/Menlo_HCO_BestPractices%20v2.pdf?t=1516815844017

[26] Wilking M. 5 Ways healthcare organizations can improve data security, July 10th, 2018, [Internet], https://www.beckershospitalreview.com/healthcare-information-technology/5-ways-healthcare-organizations-can-improve-data-security.html

[27] Attack Surface: Healthcare and Public Health Sector, Executive Overview, US Department of Homeland Security, National Cybersecurity and Communications Integration Center, BULLTIN, 10 p.,

[Internet], https://info.publicintelligence.net/NC-CIC-MedicalDevices.pdf

[28] Strategija za stalno unapređenje kvaliteta zdravstvene zaštite i bezbednosti pacijenata, "Sl. glasnik RS", br. 15/2009.

[29] Strategija za bezbednost pacijenta Agencije za akreditaciju zdravstvenih ustanova Srbije (AZUS), AZUS, Beograd, 6 str, 2010.

[30] Simić S. Pokazatelji kvaliteta rada i pokazatelji bezbednosti pacijenata u bolnicama u Evropi i svetu – Kritički osvrt i predlozi novih pokazatelja, Institut za socijalnu medicine Medicinskog fakulteta Univerziteta u Beogradu, PPT prezentacija, 34 slajda, 2013.

[31] Ćirić Z. i dr, Neželjeni događaji i pojam profesionalne greške u sestrinskoj praksi, *Nacionalni časopis Vizija*, No.2, str. 25-28, maj 2018.

[32][Internet], https://www.merriam-webster.com/dictionary/safety

[33][Internet], https://www.merriam-webster.com/dictionary/security

[34] Security checks in Serbia, Analysis of the Center for Euro-Atlantic Integration, *CEAS*, and *OSCE*, Belgrade, 46 p., June 2015. [In Serbian]

[35] The Definitive Guide to Org Charts, 52 p., [Internet], ,

[36] Trivan D, Arsenijevic O, Kastratovic E, Management of organizations in Serbia from the aspect of the maturity analysis of information security, Faculty of Business Economics and Entrepreneurship, *International Review*, No.3-4, pp. 42-50, 2016, [Internet], https://scindeks-clanci.ceon.rs/data/pdf-/2217-9739/2016/2217-97391604042T.pdf

[37] 2019 STATE OF SECURITY OPERATIONS UPDATE, 16 p., [Internet], https://content.microfocus.com/state-security-operations-2019-tb/2019-state-security-ops?lx=udA_0U?utm_source=techbeacon&utm_medium=techbeacon&utm_-campaign=00134846

[38] Romeo Ch. 6 ways to develop a security culture from top to bottom, [Internet], https://techbeacon.-com/security/6-ways-develop-security-culture-top-bottom

[39] Stuart S. Redefining Security Leadership in a Riskier World, 7 p., [Internet], https://www.spencerstuart.com/-/media/pdf-files/research-and-insight-pdfs/redefining-security-leadership-in-a-riskier-world_19aug2010.pdf

[40]Briggs R., Edwards Ch. The Business of Resilience – Corporate security for the 21st century, DEMOS, London, 109 p., 2006.

[41] Komarčević M, Pejanović Lj, Živanovic C, *Corporate Security*, Belgrade, 76 p., 2012.

[42]Roche Guidelines for the Assurance of Safety, Security, Health and Environmental Protection, 48 p, 2014.

[43] Pintarić M, Uloga i važnost korporativne sigurnosti u poslovanju poduzeća, Diplomski rad, Međimursko veleučilište u Čakovcu, Čakovec, 63 str, 2015. The role and importance of corporate security in company business, Diploma thesis, Međimurje Polytechnic in Čakovec, Čakovec, 63 p., 2015. [In Croatian]

[44] Marković S.I. Corporate Security Philosophy, *CIVITAS*, No. 7, pp. 9-22, 2014.

[45] Perčin A, Corporate Security in the Function of Risk Management, in *Proce. of IV International Conference DAYS OF CRISIS MANAGEMENT*, Velika Gorica, Croatia, pp. 359-373, 25 - 26 May 2011. [In Croatian]

[46] Pendić Z, Jakovljević B, Milinković M. Water as a strategic resource of Serbia - how to ensure the safety and quality of drinking water, in *Proc.of SORLOG 2015*, Belgrade, pp. 569-579, November 10, 2015. [In Serbian]

[47] Pendić Z, Strižak M, Jakovljević B, Polak S, Milovanović V, Jovanović Lj, Jovanović D, Lačnjevac Č, Milinković M, Beriša H, Protection of water supply systems - security aspect, in *Proc. of the VIII Scientific-Professional Conference Laws and Regulations in the world and in our country in the field of planning, design, construction and protection of space*, Belgrade, pp. 168-181, May 27, 2016. [In Serbian]

[48]Gleick PH. Water and terrorism, *Water Policy*, Vol. 8, pp. 481–503, 2006.

[49]Kroll D. J, The Terrorist Threat to Water and Technology's Role in Safeguarding Supplies, Erice, Italy, 20-23 August 2012. [Internet], http://www.-federationofscientists.org/PlanetaryEmergencies/Seminars/45th/

[50]Spencer R. Muslim hackers infiltrate water utility's control system, change levels of chemicals used to treat tap water, [Internet], https://www.jihadwatch.-org/2016/03/muslim-hackers-infiltrate-water-utilitys-control-system-change-levels-of-chemicals-used-to-treat-tap-water

[51] Strižak M, Kolarović D, Pendić Z, Jakovljević B, Makuc Z, Lačnjevac Č, Urošević S, Jovanović Lj, Jovanović D, Terrorist threats to water supply systems and approaches to their protection, in *Proc. of the Waterworks and Sewerage '16*, Vrdnik, p. 348-357, 11-14. October 2016.

[52]Chudzicki J. Current threats to water supply systems, Proc. of the 3rd International Conference on Design, Construction, Maintenance, Monitoring and Control of Urban Water Systems (UW 2016), San Servolo, Venice, Italy, pp. 1-14 (Urban Water Systems and Floods), 27-29 June 2016.

[53]Protecting the Water Sector from Security Threats: The Emerging Legal and Policy Frameworks, APWA, AMWA, NACWA, and WEF, USA, 84 p., 2007.

[54]Roadmap to Secure Control Systems in the Water Sector, WSCC-CSWG, USA, 48 p., 2008.

[55]Birkett D. M, Water Critical Infrastructure Security and Its Dependencies, *Journal of Terrorism Research – JTR*, Volume 8, Issue 2, pp. 1-21, May 2017.

[56]Fife B. Water-supply terrorism: How likely is a contamination attack?, *Georgetown Environmental Law Review*, [Internet], https://gelr.org/2016/-11/30/water-supply-terrorism-how-likely-is-a-contamination-attack/

[57]Guidelines for the Physical Security of Water Utilities, ASCE/AWWA Draft American National Standard for Trial Use, ASCE, AWWA, and WEF, USA, 2006.

[58]Luiijf E, SCADA Security Good Practices foe the Drinking Water Sector, *TNO report*, The Hague, 35 p., March 2008.

[59]Prislan K. Efficiency of Corporate Security Systems in Managing Information Threats: An Overview of the Current Situation, *VARSTVOSLOVJE, Journal of Criminal Justice and Security,* Year 16, No. 2, pp. 128–147, 2014.

[60]Corporate security & safety market in Russia, FINPRO ry, 113 p., May 2010

[61] Basara M, Nastić S, Benchmarking in Corporate Security, *MILITARY MAGAZINE*, No.2, pp. 118-145, 2015. [In Serbian]

[62]Van Leuven L. J. Water/Wastewater Infrastructure Security: Threats and Vulnerabilities, Chapter 2 in Clark R. M, Hakim S, Avi Ostfeld A, (Editors) Handbook of Water and Wastewater Systems Protection, *Springer New York*, 544 p., 2011.

[63]Albrechtsen E. Security vs safety, NTNU – Norwegian University of Science and Technology, August 2003, 8 p., [Internet], https://www.iot.ntnu.-no/users/albrecht/rapporter/notat%20safety-%20v%20security.pdf

[64]ISO/IEC 27001:2013: Information technology – Security techniques – Information security management systems – Requirements, *ISO, Geneva, Switzerland*, 2013; SRPS ISO/IEC 27001:2014: Informacione tehnologije – Tehnike bezbednosti — Sistemi menadžmenta bezbednošću informacija – Zahtevi, *Institut za standardizaciju Srbije, Beograd,* 2014.

[65]ISO/IEC 27002:2013: Information technology – Security techniques – Code of practice for information security controls, *ISO, Geneva, Switzerland*, 2013; SRPS ISO/IEC 27002:2015: Informacione tehnologije – Tehnike bezbednosti – Pravila prakse za kontrole bezbednosti informacija, *Institut za standardizaciju Srbije, Beograd*, 2015.

[66]ISO 9001:2015: Quality management systems – Requirements, *ISO, Geneva, Switzerland,* 2015; SRPS ISO 9001:2015: Sistemi menadžmenta kvalitetom – Zahtevi, *Institut za standardizaciju Srbije, Beograd*, 2015.

REZIME

GDE JE MESTO KORPORATIVNE BEZBEDNOSTI/SIGURNOSTI U ORGANIZACIONOJ STRUKTURI ORGANIZACIJE – JEDAN PRISTUP

Pojmovi „Bezbednost“ i „Sigurnost“ se prečesto koriste kao sinonimi u mnogim jezicima. Ali, bezbednost i sigurnost ne znače isto. Za bezbednost/sigurnost poslovnih procesa i zaštitu poslovnih interesa bilo koje organizacije od velike je važnosti da menadžment te organizacije razume razliku između ova dva pojma. Takođe, menadžment organizacije bi trebalo da dobro definiše zadatke i mesto(a) sistema bezbednosti/sigurnosti u organizacionoj strukturi. Sistem bezbednosti/sigurnosti organizacije trebalo bi da se posmatra kao sistem duboko povezan sa svim delovima poslovnog sistema.

Značaj sistema bezbednosti/sigurnosti u unapređenju celokupnog poslovnog sistema organizacije sve se više razume u srpskim organizacijama, jer dobro uspostavljen sistem bezbednosti/sigurnosti značajno smanjuje rizik od potencijalnih poslovnih gubitaka bilo koje vrste. Da naglasimo, ako top menadžment organizacije ima dilemu da li da uspostavi sistem bezbednosti/sigurnosti ili ne, možemo da preporučimo: Uspostavite, isplati se!

Ključne reči: *bezbednost, sigurnost, poslovni sistem, organizaciona struktura*