American Journal of Management Science and Engineering
2021; 6(6): 224-230
http://www.sciencepublishinggroup.com/j/ajmse
doi: 10.11648/j.ajmse.20210606.17
ISSN: 2575-193X (Print); ISSN: 2575-1379 (Online)

Management of Security Processes in Information Technologies

Dragan Vucinic

Department of Economy and Finance, Modern Business School, Belgrade, Serbia

Email address:
prof.dv@mts.rs

To cite this article:
Dragan Vucinic. Management of Security Processes in Information Technologies. *American Journal of Management Science and Engineering*. Vol. 6, No. 6, 2021, pp. 224-230. doi: 10.11648/j.ajmse.20210606.17

Received: June 16, 2021; **Accepted**: June 25, 2021; **Published**: December 31, 2021

Abstract: Confronted with challenges of the Information Technology, the companies have recognized the need to strengthen the resilience of its systems and structure – to strengthen cyber culture and security through continuous innovation and adjustment of the regulatory framework. The improvement of institutional capacities as a whole and continuous monitoring, evaluation and control of organizational and operational responses to cyber challenges is crucial. The goal is to establish a balance between available opportunities and the capacity for proactive performance on the one hand, and dynamic, complex and hard-to-predict cyber threats and risks, on the other. The main cause of these obstacles is definition of information security. Every sector, company must make definition of information security itself. In that way significance of information security will be raise on higher level. When we appreciate information security we may expectation better results in this aria. We need preventive control, data encryption, electronic signatures, monitoring system, control of employs, control archiving system. Finding new strategies and unique programs that will timely and effectively respond to security challenges, risks and threats and enable information technology users to live in an ever-changing world is an imperative of modern society. When it's about Serbia as a developing country, if we would observe the context of ultra-dynamic technological changes and globalization of economic flows, several questions stand to be dominant. Security of information as a key parameter affects business risks and therefore stands out as a very important factor. Preserving the confidentiality, integrity and availability of information is providing a way of accessing confidential information only to authorized persons. Integrity is maintaining the consistency of information and certifying that information is not altered. Availability certifies that information is always available when needed. The impact that losses of confidentiality, integrity and availability of information may have on assets can be critical to the organization.

Keywords: Confidentiality, Cyber-Attacks, Digital Technologies, ICT Systems, Security Processes, Security Risk

1. Introduction

Digital technologies, when observed as part of a complex global environment, have turned out to be a kind of threat to digital business as a model, given that the unlimited possibilities of technology give unlimited possibilities of technologically based abuses, which has become a constant threat and causes an imbalance in the relationship between technological innovations and their application on the one hand and the accompanying protective mechanisms and security challenges on the other.

When it's about Serbia as a developing country, if we would observe the context of ultra-dynamic technological changes and globalization of economic flows, several questions stand to be dominant. Security of information as a key parameter affects business risks and therefore stands out as a very important factor. Preserving the confidentiality, integrity and availability of information is providing a way of accessing confidential information only to authorized persons. Integrity is maintaining the consistency of information and certifying that information is not altered. Availability certifies that information is always available when needed. The impact that losses of confidentiality, integrity and availability of information may have on assets can be critical to the organization.

Preventive controls, such as the use of firewalls, access control methods, data encryption and communications, electronic signatures, data archiving systems, intrusion detection systems or monitoring systems, were the basic components of the security architecture. Typically, technical controls are complemented by a series of safety policies,

procedures, and instructions to control activities of employees.

A uniform (almost algorithmic) approach, however, proved to be insufficient. Security incidents continue to grow, and the problems of security of information resources remain unresolved. Consequently, it poses a new challenge to specialists in the field of information protection to together with company management bodies effectively consider the value of information security.

The cause of these problems may be the very definition of information security. In practice, there is a lack of consistency in the fact that each sector, industry or company, as a rule, in a uniform way defines the security of information regardless of the specifics of business needs. Such an approach has contributed to a lack of understanding and respect for the role of information security.

2. Management of Information Systems Security (ISS)

Along with the development of information technologies and the fact that companies are accustomed to the use of these technologies, the issue of information security has become one of the most important issues in the establishment and implementation of the information systems. Increasing attacks on the integrity of information systems and company data are global problem which require a systematic response.

The Law on Information Security ("Official Gazette f RS", No. 6/2016 and 94/2017) prescribes the obligation to implement measures to protect against security risks in information and communication systems (ICT systems, systems based on information and communication technologies), where security risk means actions that expose the functioning of ICT systems and defines the responsibilities of management in use of ICT systems.

Reformed data protection legislation therefore provides a number of mechanisms for flat international data transfer. The main purpose of these rules and mechanisms, not only at the level of nation, but also at the level of the EU, is to ensure that the personal data of Europeans are protected at every moment of their transfer abroad. A special document of the European Commission presents a comprehensive and simplified EU framework for the exchange and protection of personal data in a global environment. [1]

ICT system is a set of all forms of technologies used to create, store and exchange information in various forms (business data, speech, sound, images, etc.). Information security envisages performing tasks such as: [2]

1) Establishing an organizational structure, with tasks and responsibilities of employees, in order to achieve information security management;
2) Achieving safety of work out-of-office and use of mobile devices;
3) Ensuring that persons using the ICT system or managing the ICT system are trained for their jobs and that they understand their responsibilities;
4) Protection against risks arising from fluctuations in jobs or termination of employment;
5) Identifying information goods and determining responsibility for their protection;
6) Classifying data so that the level of protection corresponds to the importance of the data;
7) Data carrier protection;
8) Restricting access to data and data processing facilities;
9) Provide authorized access and preventing unauthorized access to the ICT system and services provided by the ICT system;
10) Defining the responsibility of users for the protection of means of authentication;
11) Anticipating the appropriate use of crypto currency to protect the confidentiality, authenticity or integrity of data;
12) Physical protection of facilities, spaces, premises or zones in which the means and documents of the ICT system are located and the data in the ICT system are processed;
13) Protection against loss, damage, stealing or other form of endangering the security of the assets of ICT system;
14) Ensuring the correct and safe functioning of data processing facilities;
15) Data protection and data processing tools against malware;
16) Protection against data loss;
17) Storing data that may be important for the security of ICT systems;
18) Ensuring the integrity of software and operating systems;
19) Protection against abuse of technical security weaknesses of the ICT system;
20) Data protection in communication networks including devices and lines;
21) Security of data transmitted within the company, as well as between the company and persons outside the company;
22) Information security issues within the management of all phases of the life cycle of the ICT system or parts of the system;
23) Protection of data used for the purposes of testing ICT systems or parts of the system;
24) Prevention and response to security incidents, which implies adequate exchange of information on security weaknesses of the ICT system, incidents and threats;
25) Measures that ensure the continuity of work in extraordinary circumstances.

The number of cyber security threats is growing rapidly day by day, which is why professionals in this field have almost no right to make mistakes. It has become necessary to eliminate the uncertainty factor.

2.1. DDIVE Protocol

It is obligatory to have a protocol - a set of precise steps to take when faced with an imminent danger. Such a protocol can be standardized and applied throughout the organization.

DDIVE model has 5 phases and those five phases explain

its name - detection (Detect), design (Implementation), implementation (Implementation), validation (Validate) and documentation (Establish). [3]

This protocol, or security-focused incident response, allows one to consider, implement, and document all feasible options. DDIVE is adaptable and repetitive.

Detection - this is a phase in which organizations are constantly looking for vulnerabilities and ways to improve overall security. The focus is therefore on identifying security vulnerabilities and weaknesses.

Design - once the vulnerability is identified, the next step is to create a solution that will be implemented in response to the vulnerability. The research that is done at this stage can take a long time therefore it is important to check the design well before taking action.

Implementation - at this stage, it is necessary to apply the selected solution. If possible, it is best to leave the implementation to experts who have more experience in working with the chosen solution.

Validation - this phase confirms that the solution has had an effect. It is necessary to test whether the vulnerability has really been removed.

Documentation - it is important in case the same problem reappears in the future. Also, it is a good way for new employees to get acquainted with the level of security of the company.

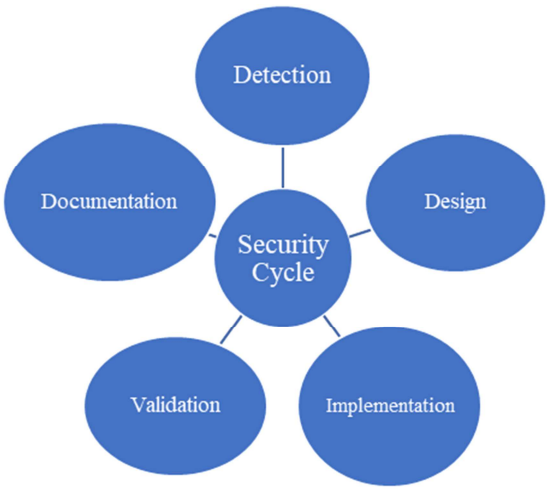

Figure 1. *DDIVE protocol.*

Although the DDIVE framework may seem too intuitive, it helps everyone in the organization to think in the same direction when it comes to security. The DDIVE model provides an information base for adequately performing security steps and documenting for future use and training.

The application of this or a similar cyber security protocol helps organizations maintain a security focus and continuously develop knowledge and expand the security database. [4]

2.2. Security Architecture Model

When it comes to information security, it is necessary to additionally consider the aspects of security. [5]

One look at a secure environment architecture that can be used to develop business solutions for any level of system specifics and complexity is given in Figure 2.

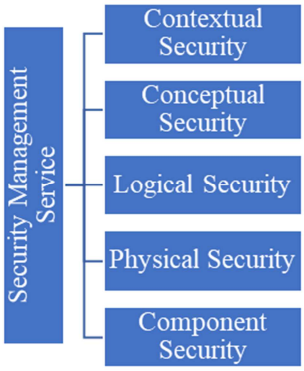

Figure 2. *Security Architecture Model.*

This business analysis is based on questions that need to be answered before starting to design a solution. These questions will help to choose a more precise solution and avoid expensive mistakes and user dissatisfaction.

The model has a layered structure as shown in the figure. Each layer contains appropriate questions defined from different points of view. [6]

The context layer should provide the business analyst with information on:

1. Business environment,
2. Classification of business assets,
3. Business motivation,
4. Processes covered,
5. Users involved in processes,
6. Locations where the solution needs to be applied,
7. Time when the solution must be available. [7]

The conceptual layer deals with the selection of logical and physical components that will be used for the later realization of the solution. With this, the business analyst determines:

1. Business risk analysis strategy,
2. Control objectives,
3. Mapping process environment,
4. IT architecture strategy,
5. Shareholder roles and responsibilities.

The logic layer helps the business analyst to determine:

1. An overview of IT assets,
2. Risk management policies,
3. Procedures for using IT services,
4. Entities and trust models,
5. Connections and data flows between locations,
6. Event schedules. [8]

In practice, the contextual and logical layers are the most difficult and only few organizations can show the factual situation. The reason for this is that very often IT departments do not have a catalog of business services and an appropriate configuration management system with details of all IT assets.

The logical model ensures that the solution can meet business goals and it is realistic from an engineering perspective. The logical model of information security is translated into a series of physical security mechanisms.

The component level focuses on an active approach to ensure that all parts fit together and function as intended. The logical and physical layer through the collected information complements the component layer and helps the business analyst to understand:

1. IT products (business applications, servers, databases),
2. Risk analysis,
3. Tools for monitoring, recording and reporting,
4. Protocols used in business processes,
5. User roles, their functions, actions and access permissions.

The final layer is a system security management service that deals with the ongoing maintenance of solutions and built-in security mechanisms in the production environment.

3. BMIS - Business Model of Information Security

The business model of information security can be presented in several ways and one of the views is shown in Figure 3.

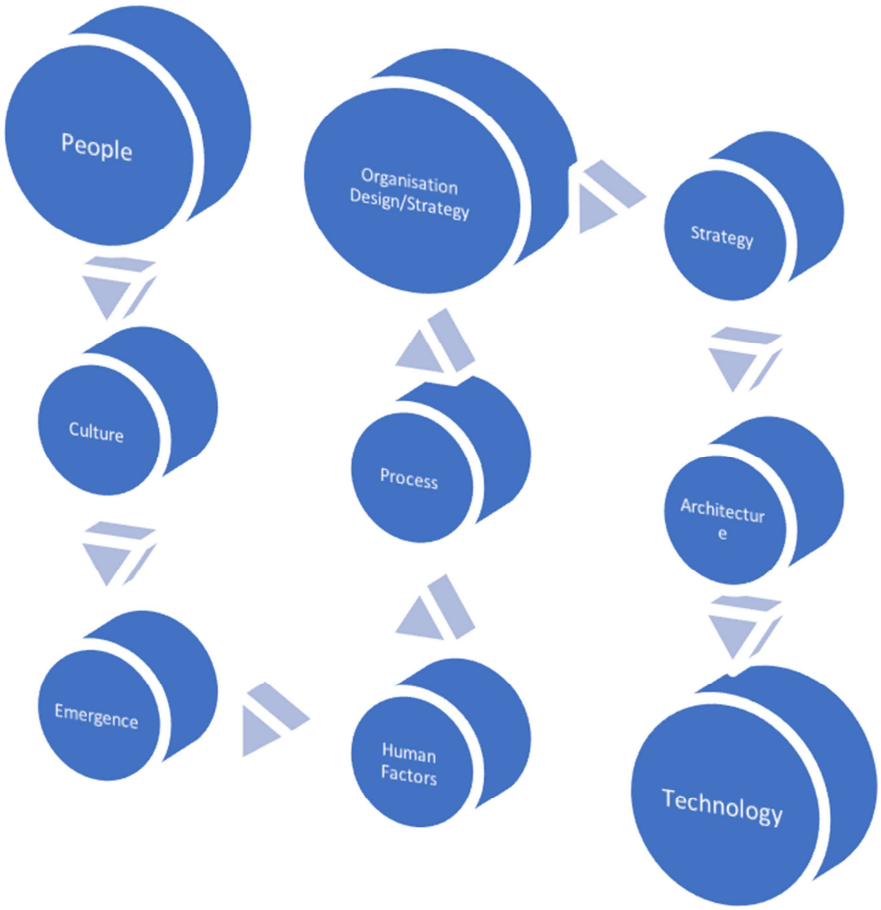

Figure 3. *Business Model of Information Security.*

Organization design and strategy - An organization is a network of people, assets and processes interacting with each other with defined roles and a common goal.

People - People represent human resources and the security issues that surround them. This determines who implements (through design) each part of the strategy. It also represents the human factor and their values; behavior and prejudices must be taken into account.

Process - The process involves formal and informal mechanisms (large and small, simple and complex) to get the job done.

Technology - Technology is an element that consists of all the tools, applications and infrastructure that make processes efficient.

In order to understand the work of BMIS in practice, it is important to study the connection between organizational structure and strategy, people, processes and technology. [9]

Figure 4 shows all the relevant resources of the organization's business support system in appropriate relationships. The methodology, as a set of practices, procedures and rules used by participants in the business processes of the system is shown at the bottom of the pyramid. The shaded triangles represent the described relationships in Figure 3. Equivalent relationships can be found for all the elements shown in Figure 4: standards that determine the system (technical standards, technological standards, legal acts, norms and other regulations of the organization), hardware, software and data.

All the elements shown in Figure 4 are in the "service" of the document, which in the figure has a central place in the

business system and to which, in essence, information security models are applied. It is clear from the picture that if we want to implement information security, we must take into account all system resources and that all system resources are of equal importance for the realization of information security of the business system.

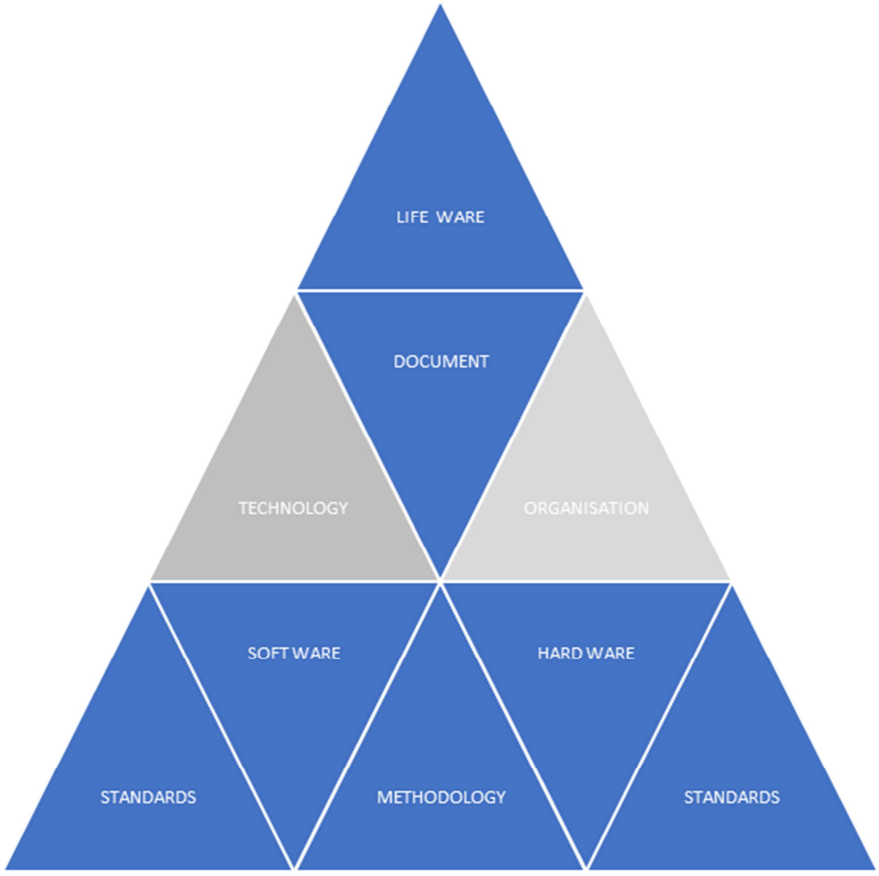

Figure 4. *Extended business model of information security.*

4. Comprehensive Protection as the Basis of Information and Security Culture

At the elementary level of system protection, it is necessary to apply: normative measures, crypto-logical measures, logical measures and physical-technical measures. [10]

Measures of a normative character, which include legal, organizational and personnel measures, belong to the category of non-technical measures. The main characteristic of these measures is that they do not degrade the operation of the system, but, on the contrary, significantly contribute to increasing its availability and productivity, and at the same time significantly affect the efficiency of the protection system. These measures establish a protection policy ("house rules"), which determines what is considered acceptable and what the sanctions are for unacceptable behavior. This gives them the character of an independent and effective instrument in the direction of preventive deterrence from illegal activities, while at the same time they represent the cheapest and most effective means of preventing and detecting numerous illicit behaviors and activities. [11]

1) Legal measures include the following:
   a. Legislation (national, Council of Europe, United Nations…);
   b. Internal acts, regulations, rules and other documents;
   c. Safety risk assessment act;
   d. Protection of privacy and intellectual property;
   e. Sanctioning all types of cybercrime.
2) Organizational measures include standards, mission vision and objectives, security policy, code of implementing and security procedures for access control.

The most important standards are ISO, NIST, CRAMM, EBIOS, OCTAVE, HIPAA, COBIT, ITIL, FISAP, FISMA and others. The organization should follow all safety recommendations given in international and best practice standards, and in particular the provisions relating to the threat to human rights, privacy and identity of employees and other stakeholders, as well as the threat to copyright and licenses. Mission, vision, goals are the "holy trinity" of every organization. Based on these documents and its own needs, the organization defines the security goals that it sets for its employees.

Security policy [11] declares the obligation of the organization to make security affairs its priority. It provides a framework for best practice that can be understood and

followed by all employees, which crucially helps to ensure minimized risk and to respond effectively to any security incident. The general requirements and recommendations of the security policy include the following:

1. The organization is the owner of all information assets, as well as all processes and electronic transactions;
2. Raise the level of protection and maintenance to the highest possible level using all the recommendations of security experts and manufacturers of IT hardware and software, as well as all available means;
3. Management is responsible for establishing and implementing standards and procedures, as well as for controlling access to the organization's information assets and controlling access to Internet and intranet users; personal example management should demonstrate and support raising users' awareness of the need to protect information assets, as well as prepare users for self-protection and reduction of cybercrime risk through various levels of training;

The Code of Business Ethics, with a special emphasis on information security, is a document that applies to all employees and whose purpose is to instruct them on how to adapt their behavior to the work environment, in accordance with moral and professional norms and generally accepted values. The code should contain the following elements: attitude towards business and associates, attitude towards clients and business partners and attitude towards assets.

Security procedures for access control refer to use of passwords, e-mail, antivirus protection, social networks, visits to sites and downloads of programs and files, all the way to the procedure for backing up data, procedures in case of danger and security incident, as well as treatment procedures risk.

5. Resilience to Cyber-attacks

Generally, the goal is to ensure greater resilience, strategic independence and ability of the company to develop and apply technologies and skills to enhance cyber security. To strengthen cyber resistance, a common and comprehensive approach is required, as alleged.

In practice, this implies more robust and more efficient structures for the development of cyber security and a more effective response to cyber-attacks.

In this regard, the key priority of the reform of the legislative and institutional framework, in the field of cyber security is the institutional strengthening.

In order to establish resilience to cyber-attacks and as a single market in the cyber security field, it is necessary that all relevant actors, that is, state bodies, economic operators, owners and operators of network infrastructure, focus all their activities on the next three priority areas:

1. Security in key or high-risk areas, i.e. systems.
2. Cyber security in digital products, networks, systems and services of wide use in the private and public sector for the purpose of defense and protection against attacks and implementation of regulatory obligations e.g. e-mail encryption, firewall protection, and virtual private networks.
3. Using "integrated security" methods in affordable, digital, interconnected broadband devices that make up the Internet of Things.

General Data Protection Regulation (GDPR) is the fundamental Europe's digital privacy legislation. It represents a set of rules designed to provide EU citizens more control over their personal data and its safety. GDPR targets to narrow the regulatory environment for business so companies can fully benefit from the digital economy.

Under its terms, all organizations have to guarantee that personal data is collected legally and under strict conditions, and that those who collect and manage personal data are obliged to protect it from abuse and exploitation, or face severe penalties in case of disrespect.

6. Conclusion

Information security is a core value of the organization and significantly contributes to the security of each system only if it is designed and implemented on time and as a fundamental part of the business strategy.

Information security is a prerequisite for building trust in an organization in order for it to gain and retain business customers, and thus achieve business goals. To define information security within an organization, business objectives must first be understood, all key actors and resources identified, and linked to information security models. The role of the business analyst is crucial in the stated tasks of defining and implementing information security in each organization.

Finding new strategies and unique programs that will timely and effectively respond to security challenges, risks and threats and enable information technology users to live in an ever-changing world is an imperative of modern society.

References

[1] Čelik P. (2019). Institutional Measures for Enhancing Business Cyber Security in the European Union, Економске теме, ISSN 0353-8648 (eISSN 2217-3668), UDK33 (497.11). Niš, oktobar 2019.

[2] Danchev, D., Building and Implementing a Successful Information Security Policy, http://www.windowsecurity.com/pages/security-policy.pdf(20. 12.2015.

[3] http://www.windowsecurity.com/pages/security-policy.pdf (20. 12. 2015).

[4] https://positive.rs/konsalting-i-edukacija/bis-bezbednost-informacionih-sistema/

[5] Milanović, Z., Srećković, M., Znanjem protiv zloupotrebe enkripcije, Naučno-stručni skup sa međunarodnim učešćem "Suprostavljanje savremenim oblicima kriminaliteta – analiza stanja, evropski standardi i mere za unapređenje", Zbornik, Tom 3, Tara, 2015, pp. 135–147.

[6] Pejanović Lj., Komarčević M., Čelik P. (2017). Centralizacija i militarizacija područja bezbednosti u Evropskoj Uniji, Crisis Management Days, 10th International Scientific Conference, Velika Gorica.

[7] Petrović, S., Zaštita računarskih sistema, Viša železnička škola, Beograd, 2004.

[8] Swanson, E., Ramiller, N. "The organizing vision in information systems innovation", Organization Science 8 (5), 1997, pp. 458–474.

[9] Social Inclusion and Poverty Reduction Team, 2018, The third national report on social inclusion and poverty reduction in the Republic of Serbia, https://bit.ly/2XoiPQw

[10] Western Balkans Labor Market Trends 2019, World Bank (2019b), Washington DC.

[11] https://www.batimes.com/articles/addressing-information-security-in-business-analysis-with-sabsa.html