IMPORTANCE AND SECURITY OF INFORMATION IN TERMS OF BUSINESS TIME DURING COVID 19

Miodrag BRZAKOVIĆ
Darjan KARABAŠEVIĆ
Gabrijela POPOVIĆ
Ana VELJIĆ

Abstract: *The scientific paperwork pointed out the importance of information and information systems that represent important business assets and one of the most important resources of any organization. The specificity of information protection and security in the conditions of the pandemic caused by COVID 19, requires a systematic approach in order to provide timely, reliable and accurate information. The process of information security and protection is a complex process, multidisciplinary in the function of achieving the ultimate goal, which is secure and reliable information. This approach requires reliable and secure information systems in organizations that are information carriers in the conditions of a pandemic caused by COVID 19.*
Keywords*: information, information systems, data and information security*

INTRODUCTION

Why is information protection necessary? Information and information systems are important business assets, and the confidentiality, integrity, and availability of information can be critical to maintaining all the vital functions of an organization or community (Karabašević et al., 2018).

The constant development and strengthening of dependence on information systems and services means that the organizations themselves are becoming significantly more vulnerable to security threats.

Any organization and especially organizations of special importance as well as their information systems face, with a tendency to increase, security threats from a wide range of sources endangering their security.

In contrast, many information systems are not designed to protect themselves. The level of security that can be achieved by technical means is limited and must be supported by appropriate management and

procedures. Determining the controls to be set up requires careful planning and attention to detail. In order to manage information protection, the participation of all employees in the organization is required as a minimum.

Organizational protection measures in the security system should ensure the smooth and efficient functioning of the information system, which should provide timely, accurate and reliable information. In order for the information system to be properly dimensioned and function smoothly, but also to recover quickly after a long or short "shock", there must be a defined level of critical applications and configurations in the system, how they work as well as potential weaknesses.

THE IMPORTANCE OF INFORMATION SYSTEMS SECURITY

The concept of information systems security is treated in the way it is accepted today in developed countries in the world and which ensures compliance with the concept of information security and established standards in this area.

An information systems security system includes people, processes, organization, and technology. The system should consist of a series of harmonized security measures, such as: security checks of persons, physical security, data and information security, as well as coordinated introduction of formal procedures, such as risk assessments, certification of persons and devices, as well as accreditation of technical systems for application in a certain segment of the business process of a certain organization. Compliance and coordination of important measures and procedures is achieved through the organization and management of information security.

Information systems security includes data security on electronic media and computers, data security in data transmission systems and security of information infrastructure in special categories of space, protection against misuse of social networks, portals, etc.

The security of the information system is even more important if we keep in mind their application in organizational (special) systems. These are organizational systems that are especially important for the state, highly demanding in relation to the reliability of functioning and imply that they are critical from the security aspect.

Information systems security is a dynamic process throughout the life cycle of the system that should be considered from the stage of its planning, development, implementation, operation, growth, to expenditure

and destruction as needed, with due respect for the specifics of the situation in which they operate.

Such a process requires a high-quality approach to risk management processes used to assess, monitor, eliminate, avoid or accept risk. Risk management is a skill that balances the costs of applying additional security countermeasures and the benefits that result from them. The purpose of the risk management process is to ensure the permanent functionality of the security objectives of confidentiality, integration and availability of data.

In general, it can be said that the security of information systems includes everything that information security in a broader sense, only applied in a narrower technological framework, which should include not only the individual but the entire system of one society.

The life cycle of an information system inevitably accompanies security-related documentation. It implies interaction between all parties involved in the operation of information systems, from users through the members responsible for planning, implementation and operation (security study, plans for operational use of the system, etc.).

INFORMATION SECURITY MANAGEMENT IN A PANDEMIC

The pandemic of the disease caused by the corona virus (COVID-19) (WHO) of unprecedented proportions. The spread of the virus takes lives and affects the main resources of families struggling to survive, as well as the quality of life itself.

Communities are responding to the challenge - from health workers risking their lives to fight the virus, to young people sharing messages about public health in innovative ways. However, although the spread of the virus is slowing down, its social consequences will come quickly and it will be difficult.

In order to respond to the urgent needs required to respond in such situations, it is necessary to redistribute the priorities of its internal resources. The most important resource in such situations is information and knowledge on how to react in a timely and correct manner.

Information represents certain assets, which, like other important business assets, have value for an organization and therefore need to be adequately protected (ISO/IEC 27001:2015; Kiilu & Nzuki, 2016). Information security protects vital functions from a wide range of threats in the business continuity function, or to minimize business losses.

The basic goals of information security management are to enable the organization to realize its mission and business activities while taking care to avoid, or minimize risks related to business information security that could endanger the interests of the organization or its stakeholders.

Information Security Management System – ISMS is a set of interrelated activities, methods and techniques that ensure the confidentiality, availability and integrity of information from all threats to them (Kukrika, 2002).

In order to achieve information security, it is necessary to meet the key requirements related to security:

a) confidentiality: ensuring that information is available only to those who have been granted access to the information;
b) integrity: self-protection of accuracy and completeness of information and processing methods;
c) availability: by ensuring that authorized users have access to information and associated assets when they need it.

In order for the information to have the required level of security, it is necessary to strictly meet the stated requirements, as shown in Picture 1.

In order to ensure the required security of information, it is necessary to create appropriate conditions by introducing a suitable set of management controls, which can be the policy of the organization. These procedures should be established to ensure that the organization meets specific protection objectives.

Successful implementation of information security within organizations (communities) of a company, or in general within any business organization, requires systematic management of various aspects of information security, supported by an appropriate legal framework. Precisely because of the importance and the need to harmonize procedures and information security procedure, and in order to achieve interoperability, information security management must be harmonized with the organizational hierarchy and in accordance with the prescribed organization at the national level.

To secure interoperability all information security regulations should be they should be submitted on the highest executive level, whether by the state or an organization as a business entity. In this way, mandatory application is ensured these acts at all hierarchical organizational levels, which enables the achievement of minimum-security criteria of the entire system. The process of information system security management is responsible for the continuous improvement of the legal framework, starting from the security policy, through the planned regulations, rules and

guidelines, to the detailed procedures of individual bodies organized at all levels.

The modern approach to information security management is multidisciplinary and includes a number of aspects:

- strategic management dimension,
- management/organizational dimension,
- political dimension,
- the best practice dimension,
- ethical dimension,
- certification dimension,
- criminal dimension,
- insurance dimension,
- personal/human dimension,
- training dimension,
- technical dimension,
- measurement/metric dimension (compliance control) and
- the audit dimension.

INFORMATION SYSTEM SECURITY MANAGEMENT

Information system security management includes procedures such as: provision of resources, data classification, risk management measures, planning and implementation of measures, control of implementation and applicability of measures and procedures, ensure continuity of the information system. This procedure also requires the training of all participants in the system of providing timely information in the conditions of COVID 19.

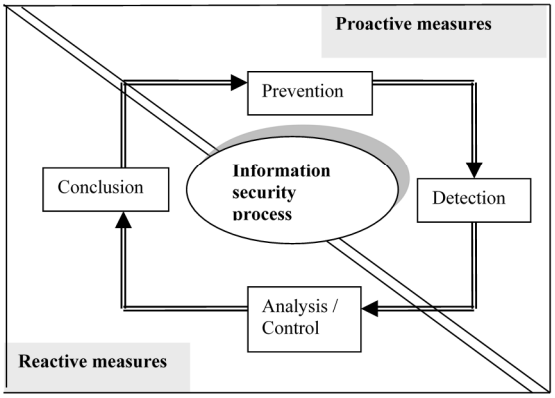
Information security management in computer systems can be conditionally divided into two parts - proactive and reactive action.

Proactive measures are those that are applied "before security incidents" and aim to prevent incidents. The goal of incident response planning is to reduce the risk of security and functionality of the information system in incident situations in providing practical recommendations for optimal handling when incidents occur. Adequate incident response planning increases an organization's ability to respond successfully and quickly to incidents, to limit and correct damage, and to reduce the consequences of future incidents. Assumption for successful planning of responding to incidents is a good knowledge of the information system environment as well as one's own system, which refers to knowing and monitoring potential threats, on the one hand, and knowledge of information system vulnerabilities on the other hand.

This part must represent the essence of the information security system, and consists of security policy and prepared acts, organizational and technical norms, risk assessment and management, periodic audit processes, etc.

Reactive measures are those applied "after the occurrence of security incidents" and aim to assess and recover from damage caused by security incidents, reviewing the organizational and technical parts of the system for the purpose of future prevention of similar incidents, as well as conducting the collection of evidence for the detection and legal prosecution legal prosecution of the perpetrator of a particular security incident.

A well-organized information system security management system in the conditions of a pandemic has a direct preventive impact on the overall security situation of the country, which forms the basis for the development of essential repressive procedures of the modern information society.



Picture 1: Process review for information security
Source: Petrović (2005)

RISK MANAGEMENT IN THE FUNCTION OF INFORMATION SYSTEM SECURITY

The success of all organizations depends on the availability and proper functioning of a wide range of complex information systems and obtaining answers based on the principle of so-called "golden rules":

- WHAT to protect?
- FROM WHOM or FROM WHAT to protect?
- WHY protect?
- WHAT to protect WITH?

- HOW to protect?

The ultimate goal is:

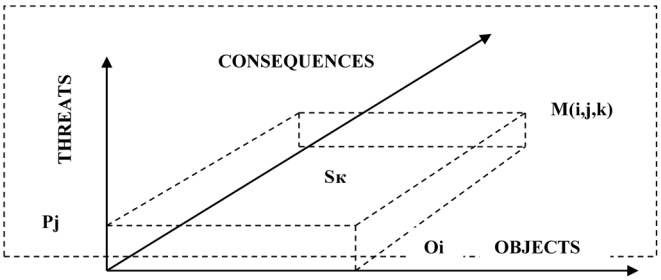
- How to see the level of vulnerability of the system or the degree of protection of the system..
- How to see the level of importance of the system depending on the financial, material or political value of the system.
- Choice of risk assessment method (whole organization or by its parts).
- How to define the control mechanism in the function of risk management.

In order to find and develop a unified and comprehensive approach, which should provide a reliable basis for ensuring interoperability in the field of security measures and procedures, which requires organized, professional, rational and designed study and resolution of this issue (Brzaković, 2009).

The answer to the first question (WHAT to protect?) implies the determination of the objects of protection, to the second question (FROM WHOM or FROM WHAT to protect?) implies the identification of threats (dangers) which, to a greater or lesser extent, may jeopardize protection facilities, to the third question (WHY protect?) implies determining the consequences that a threat may cause in relation to an object, to the fourth question (WHAT to protect WITH?) implies the choice of measures to be used, and to the last question (HOW to protect?) implies defining protection policy.

We should start from the fact that no information system can be absolutely secure and to that end it is necessary to consider all the risks that threaten it and how to reduce the possibility of their occurrence (Petrović, 2005).

Accordingly, the main entities of protection problems in the field of information systems are objects of protection, threats, consequences and measures. This approach allows the problem of protection, for clarity and easier observation of existing interdependencies, to be presented in the form of a three-dimensional matrix, where each element of the matrix M (i, j, k) represents a set of measures that should be applied to prevent consequence S (k), which can occur if the threat P (j) threatens the object O (i), ie. mz = m (Oi, Pj, Sk), picture 2.



Picture 2: Three-dimensional matrix of interdependence of threats, consequences and objects (Source: Petrović S .: "Computer crime", MUP RS, Belgrade, 2005, page 10)

This approach allows the problem of protection, for clarity and easier observation of existing interdependencies, to be presented in the form of a three-dimensional matrix, where each element of the matrix M (i, j, k) represents a set of measures that should be applied to prevent consequence S (k), which can occur if the threat P (j) threatens the object O (i), ie. mz = m (Oi, Pj, Sk).

ELEMENTS OF RISK MANAGEMENT

Risk assessment is the most important step in risk management and it represents two basic attempts that are reflected through: qualitative assessment and quantitative assessment.

Qualitative assessment is realized through surveys and joint gatherings, which include people from different parts of the organization. Purpose of these analyzes is to establish which measures have already been implemented and to assess their value. It then attempts to establish what threat may be encountered and what types of vulnerabilities may be exploited in the future. Based on the obtained indicators, a selection of measures is made with the intent of reducing the risk within the allowed funds and possibilities of a certain organization (Security Risk Management Guide).

Quantitative risk assessment is an attempt to calculate the actual numerical value for each of the elements collected during the risk assessment (e.g., loss of productivity, reputation, etc.) as well as the benefit of the analysis (Tipton & Krause, 2004).

CORONA VIRUS AND ONLINE SECURITY

Information systems that monitor Covid-19 in order to carry out epidemiological surveillance during an epidemic, must implement all prescribed measures relating to information security and data protection of individuals (Adamović [et al., 2020]) as well as to properly provide information of public importance.

Health care institutions, public health institutes and institutes, testing laboratories and other competent authorities enter data on the cured, deceased, tested and persons who have been sentenced to self-isolation into the information system, and take into account the manner of access to information and data arising from their system. This data, through the website of a health institution, and with the help of the username and password that were available on it, defines the right of access. One of the basic protection measures is to prevent unauthorized access. Disrespect with the standards of security and protection of data and information in the public health system, affects the suspicion of what is actually happening with our data.

It is necessary to provide a mechanism for authenticating system users based on a high level of reliability scheme, by using a qualified electronic certificate. The use of the certificate should ensure high confidence in the identity of the person, prevent abuse and provide prevention of incidents.

CONCLUSION

In order to protect systems from the negative effects of any form of Covid-19 safety and to provide the necessary conditions for the functioning of the organization in the conditions of a pandemic caused by survival and in the most difficult working conditions, it is necessary to provide key features such as:

- Adequate measures to ensure resistance to attacks on the organization's information system;
- Timely recognition of attacks and extent of damage;
- Procedure for recovery of complete and basic services after the attack and
- Manner of adaptation and development in order to prevent the effectiveness of future attacks on the individual, organization, etc.

Due to their functional and physical characteristics, computer systems are exposed to many dangers, where the vulnerability of these systems is particularly pronounced in the conditions of emergencies caused by the pandemic caused by Covid-19. The realization of the ability to survive in such conditions is a very complex problem whose solution requires significant

engagement of all segments of society and organizations of the owners of a particular system.

References

Adamović, J. , Krivokapic, D.,Tasić, D., Kleut, J., Nicovic, N., Kalajdzić, K., Mileusnić, M., & Krivokapić, Dj. (2020). A guide to protecting personal data during a pandemic. White City.

Brzakovic M. (2008). Interoperability and information security in organizations of strategic importance in emergency situations. Doctoral dissertation, Belgrade.

ISO/IEC 27001:2015 - Information security management.

Karabašević, D., Stanujkić, D., Brzaković, M., Maksimović, M., & Jevtić, M. (2018). Importance of vulnerability scanners for improving security and protection of the web servers. Bizinfo (Blace), 9(1), 19-29.

Kiilu, K. P., & Nzuki, D. M. (2016). Factors affecting adoption of information security management systems: a theoretical review. International Journal of Science and Research (IJSR), 5(12), 162-166.

Kukrika, M . (2002). Information Security Management - Protection of information systems according to ISO 17799. INFOhome Press, Belgrade.

Petrović, S . (2005). Computer Crime. RS Ministry of the Interior, Belgrade, 9-10.

Security Risk Management Guide (2004). Microsoft Corporation, 16-20. http://www.microsoft.com/technet/security/topics/complianceandpolicies/secrisk

Tipton, H., Krause, M. (2004). Information Security Management Handbook. CRC Press, London, 1185 -1189.

World Health organization, WHO.

NOTES ON THE AUTHORS

Miodrag BRZAKOVIĆ, Ph.D., is a Professor and Council President at the Faculty of Applied Management, Economics and Finance, University Business Academy in Novi Sad. E-mail. miodrag.brzakovic@mef.edu.rs

Darjan KARABAŠEVIĆ, Ph.D. is a Vice-dean for Scientific Research and an Associate Professor of Management and Informatics at the Faculty of Applied Management, Economics and Finance, University Business Academy in Novi Sad, Serbia. E-mail. darjan.karabasevic@mef.edu.rs

Gabrijela POPOVIĆ, Ph.D., is an Associate Professor at the Faculty of Applied Management, Economics and Finance, University Business Academy in Novi Sad, Serbia. E-mail: gabrijela.popovic@mef.edu.rs.

Ana VELJIĆ, Associate teacher at the Faculty of Management, Economics and Finance, University Business Academy in Novi Sad. Faculty of Applied Management, Economics and Finance in Belgrade, Jevrejska 24, 11000 Belgrade, Serbia; Research Associate in Social Sciences – Economics, E-mail: ana.veljic@mef.edu.rs