JOGSC
Journal of Global Science
ISSN: 2453-756X (Online) Journal homepage: http://www.jogsc.com

Information Security Management System

Antonín Korauš*
Akadémia Policajného zboru v Bratislave,
Sklabinská 1, 835 17 Bratislava 35, Slovenská republika,
antonín.koraus@minv.sk

Pavel Kelemen*
University of Prešov in Prešov
Faculty of Management,
Konštantínova 16, 080 01 Prešov, Slovakia
kelemen.pavel@gmail.com

Stanislav Backa
University of Prešov in Prešov
Faculty of Management,
Konštantínova 16, 080 01 Prešov, Slovakia
stanislav.backa@gmail.com

Jozef Polák
University of Prešov in Prešov
Faculty of Management,
Konštantínova 16, 080 01 Prešov, Slovakia
jozefpolak64@gmail.com

* corresponding author

Abstract: Networks and information systems play a crucial role in free movement and are often interconnected and linked to the Internet as a global tool. A disruption of the network and information systems in one member state therefore affects other member states and the whole European Union. The resilience of networks and stability of the information system is therefore a basic prerequisite for a smooth and undistorted functioning of the European Union's internal market and a prerequisite for credible international cooperation. The information security policy applies to every piece of information that is processed in an organization, regardless of its form or method of processing. It also applies to systems through which the information is processed, including their supporting infrastructure and persons processing the information.

Keywords: Information security, information and communication technologies, information systems, management system, security, cyber security

JEL klasifikácia: C22; C51; Q11; Q13

1. Introduction

According to the international standard ISO / IEC 27001, information security is a protection of information against a wide range of threats. Its aim is to ensure the continuity of business processes by:

- minimizing losses and
- maximizing returns on investment.

At present, the measure of electronic information being processed by means of computers and other information and communication technologies is increasing. The potential to disrupt this information, either directly or through attacking the technical devices or environment in which the information is being processed, is called a threat. There

are many factors either potentially threatening or directly disrupting information and communication technologies and degrading the information being processed within. These include, for example, natural impacts, technical failures, human errors and mistakes, malicious software, targeted attacks, cybercrime and international terrorism. All of them have the potential to bring about serious security problems.

The objectives of information security are to minimize the possibilities of threats being carried out and, in case that consequences have already occurred, to minimize their impact. These objectives are essential for both the public administration and private sphere, but especially for critical information infrastructure of a country[1].

Information security must take into account the interests and needs of owners and users of information and communication technologies as well as the rights of natural persons and legal entities whose data are processed in the systems. From the users' point of view, the most important factors in the processing of information are its purpose, content, accuracy, timeliness, accessibility, authenticity, arrangement and quality. From the point of view of owners and operators, the most important factors include the (preferably on-line) availability of information resources, and their security against information leaks unauthorized use and disruption of the integrity of the data, including the integrity of the authority and reputation of the system owner.

A failure to secure the information can result in irreparable losses and damaged reputation of the organization and state. Given that the state is a guarantor of critical processes, it has a role to play in taking care of the overall level of competitiveness of the society and thereby in protecting national wealth, including knowledge and information. Therefore, the state cannot afford to operate at a low level of security criteria. Given the potential adverse impact, it is the duty of the state to ensure the protection of information from misuse and to minimize the consequences of such misuse.

The need for information security was also recognized by national governments, supranational authorities and world-renowned organizations such as the Organization for Economic Cooperation and Development, United Nations, North Atlantic Treaty Organization, and G8 as well as international and European standardization organizations which created various institutions and institutional systems for ensuring information protection, such as the European Information Security Agency, High Level Internet Governance group, and Computer Incident Response Team. These institutions have established their strategic goals and are taking action to meet them. Many of their goals have already been achieved.

2. Legislative Basis

Based on the approved program statement of the Government of the Slovak Republic for the years 2016-2020 and in line with the approved Cyber Security Concept of the Slovak Republic for 2015-2020 and action plan for implementing the latter concept in the Slovak Republic in years 2015-2020, the National Security Authority, as the central state authority for cyber security, prepared a bill on cyber security and amendments and supplements of some laws (hereinafter “the bill”) by which a new directive is transposed into the national law, namely the

Directive 2016/1148 of the European Parliament and Council as of 6 July 2016 on measures to achieve a high common level of security of network and information systems in the European Union (hereinafter NIS Directive). The aim of the NIS Directive, as well as that of Act No. 69/2018 on Cyber Security, effective from 1 April 2018, is to ensure the protection of information systems and networks against disruption of either the technical devices themselves, data processed in them or services provided by them.

In its individual articles, Act no. 69/2018 Coll. on Cyber Security amends some legal regulations to achieve sufficient transposition. This applies specially to Act no. 198/1994 Coll. on military intelligence as amended, Act No. 319/2002 Coll. on the defense of the Slovak Republic as amended, Act no. 45/2011 Coll. on critical infrastructure,

[1] Critical information infrastructure is the means and networks of information and communication technologies, related values and electronic services whose destruction or malfunctioning as a result of the risk factor poses a threat or distorts the political and economic functioning of a state or the threat to life and population health.

Act No. 351/2011 Coll. on electronic communications, as amended, and Act No. 483/2001 Coll. on banks and on amendments to certain acts, as amended. In connection with the introduction of the new administrative fee, the Act no. 145/1995 Coll. on administrative fees has been also amended.

Act no. 69/2018 on cyber security imposes an obligation to its primary addressees, namely basic service operators and digital service providers, to meet the requirements of the latter act no later than October 1st, 2018. The identification criteria for basic service (and their operators) are set out in a respective implementing regulation (National Security Authority Regulation No. 164/2018 Coll., which defines the identification criteria of the service being operated). Digital services and their providers include online marketplaces, web search engines and cloud computing services provided by a legal entity or natural person, namely an entrepreneur who at the same time employs at least 50 employees and has an annual turnover or total annual balance of more than 10 million Euros.

In addition to other state administration bodies, the obligatory entities include the National Security Authority, Ministry of Transport and Construction of the Slovak Republic, Ministry of Finance of the Slovak Republic, Ministry of the Economy of the Slovak Republic, Ministry of Defense of the Slovak Republic, Ministry of the Interior of the Slovak Republic, Ministry of Health of the Slovak Republic, Ministry of Environment of the Slovak Republic, Slovak Information Service, Office of the Deputy Prime Minister for Investment and Informatization and Military Intelligence.

The NIS Directive is the first pan-European legislation on cyber security aimed at strengthening the competences of relevant national authorities, increasing their mutual coordination and representing security conditions for key sectors.

The aim of the NIS Directive is to guarantee a common security of networks and information systems within the European Union by enhancing the security on the Internet, private networks and information systems, on which the functioning of economic and social interests is largely based.

The European Network and Information Security Agency (ENISA) is a very important subject in the field of cyber security in the European Union. It contributes to the achievement of high level of security. In cooperation with European countries, it creates a common culture of network security and information systems in the European Union.

The Member States' obligations under the NIS Directive are set at the least acceptable level necessary to achieve the required preparedness and ensure a cross-border confidence-based cooperation. Within the framework of adopted measures, the member states may take account of their national specificities while each member state transposes the NIS Directive in the light of real risks occurring in their own society.

The main implications of NIS Directive are as follows:

- To introduce the security requirements as well as requirements for reporting cyber-security incidents to the Basic Service Provider and Digital Service Provider (hereinafter referred to as "BSP" and "DSP", respectively),
- To oblige member states to designate national competent authorities and establish integrated points of contact and teams for resolving cyber security incidents (hereinafter referred to as "CSIRT" units),
- To oblige member states to adopt their own national cyber security strategies,
- To establish a cooperation group to promote a strategic cooperation and exchange of information between member states, and build mutual trust,
- To establish a network of CSIRT units to contribute to the development of trust between member states, and promote an effective cooperation.

In line with the objectives of NIS Directive and in connection with the Legislative Purpose of the Information Security Act, which in addition to partial objectives sets out solutions to two basic areas of problems, namely those of ensuring protection for public administration information systems and establishing a general legal framework for the protection of the entire digital space of the Slovak Republic, it can be stated that the Cyber Security Bill addresses all relevant issues in a comprehensive and integral way.

The aim of the Act is to create a functional legislative framework that is essential for the effective implementation of key measures for national cyber security space, and to transpose the priorities and requirements that have been set up at European level and adopted by general consensus through the NIS Directive.

Major areas of bill amendments in line with the NIS Directive are as follows:

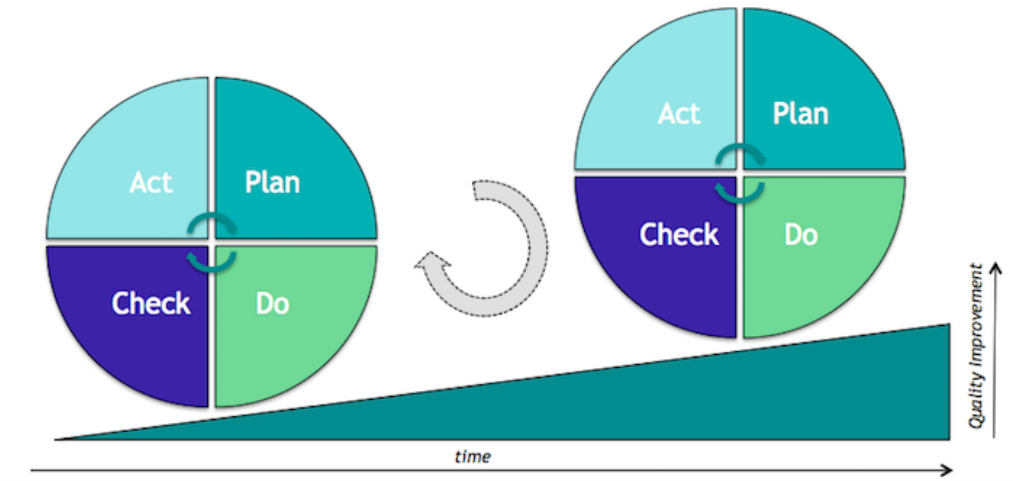
- Organizations and scope of public authorities in cyber security,
- National cyber security strategy,
- Single cyber security information system,
- Status and obligations of BSP and DSP,
- Organization and operation of CSIRT units and their accreditation,
- System securing cyber security and minimum requirements for cyber security,
- Control and audit.

In addition to those mentioned above, the Act also addresses some further requirements of the NIS Directive, such as the definition of international cooperation on cyber security, fulfillment of notification obligations, reporting of cyber security incidents as well as voluntary reporting of cyber security incidents, supporting research and education as well as increasing security awareness in the field of cyber security. In a comprehensive manner, the law further addresses employee remuneration on the part of the state so that the state can employ cyber security professionals and compete with private employers.

The information security requirements resulting from the laws briefly mentioned in the overview of legislation apply mainly to information systems processing the personal data or information systems of public administration. The range of security measures in the private sphere is not strictly required by legislation, except for those relating to personal data and, where appropriate, to the provision of electronic communication services. If a company wants to achieve a situation where full and correct data are obtained by those who need them and are eligible to access them, it is important to establish an information security management system within the enterprise.

ISMS (Information Security Management System) is part of an enterprise-wide organization management based on an approach to risk activities. It is focused on provision, implementation, operation, monitoring, review, maintenance and improvement of information security (ISO / IEC 27001: 2013). ISMS is defined by ISO / IEC 17799: 2005 and ISO / IEC 27001: 2013. According to ISO / IEC 27001: 2013, the implementation of an information security management system is seen as a project. Thus, the Deming PDCA cycle is used, while the whole project consists of four repeating steps: plan, implementation (Do), monitoring (Check), and decision-making (Act).

Figure 1 Deming cycle



Source. ICT Istitute.nl

The access to information security management must be tailored to the size of the particular organization and its nature or focus. In general, for small companies with up to 20 employees, there is no need to hire a full-time security expert. The latter need or even that of a whole department that is independent of IT department becomes relevant in larger companies. We will briefly describe a documentation related to information security management. The latter documentation analyzes the internal environment from the aspect of vulnerability of the corporate network.

3. Information Security Policy

The basic document of information security in a company is its information security policy. This document should be accepted in co-operation with business management and should include a statement that for the sake of protecting information and related assets the organization shall ensure sufficient personnel, material, and organizational and legal conditions as well as introduce mechanisms for monitoring security incidents and assessing their severity.

In their information security policy, the organization should assess the key people, their responsibilities for their level of information security in the organization as well as possible sanctions for violating their obligations.

- The main objectives of the organization in information security are as follows:
- To ensure the protection of all information assets of the organization (computers, networks, software, data, etc.) and reduce to a reasonable extent the risks arising from the disruption of confidentiality, integrity and availability of its information assets;
- To ensure that all users of information communication technologies (ICT) of the organization are aware of and carry out their obligations in line with relevant European and Slovak legislations;
- To provide a reliable and secure work environment to all organization employees and other legitimate ICT users through information and communication systems.

4. Risk Analysis

Asset classification is appropriately followed by the procedure of risk analysis. It helps to create a guiding framework for assessing the significance of vulnerability in the context of asset classification and thus facilitate the decision-making in implementing security measures and prioritizing them.

There are more ways of accessing the assessment of information security risks. Based on the approach to risk analysis, the methods are divided as follows:

- Qualitative risk analyses describe the impact and its likelihood verbally. The disadvantage of this approach is in a considerable degree of subjectivity in chosen means of expression by the evaluator, which may lead to misinterpretation of the resulting report. The disadvantage lies also in the inconsistency of such analysis, as well as in the inability to compare the analysis with those of other organizations. Qualitative risk analyses are used especially where it is not possible to evaluate probabilities or impacts numerically.
- Quantitative risk analyses use numerical values to evaluate the impact. The advantage over the qualitative risk analysis lies to some extent in the elimination of the evaluator's subjectivity. The disadvantage of this type of analysis is in the need for sufficient numerical data to evaluate the impacts and their probabilities. It is quite difficult to set the rating scale. Each successive step increases the number of combinations of impact probabilities. There are also specialized software tools for quantitative risk analyses.
- As a result of risk analysis, the risks assessed as being damaging and unacceptable, can have a significant negative impact on the business. Therefore, it is the latter category of risks that should be prioritized in the process of applying security measures in order to reduce them to an acceptable level.

4.1 Security measures for reducing the level of risk

When adopting security measures in an organization, it is also appropriate to follow the Deming methodology. The desired effect can be achieved only by strictly adhering to the process of drawing up a plan for their implementation, implementation as such, regular monitoring of its effectiveness and correction of any deficiencies.

Safety precautions must be carefully chosen in the plan following the risk analysis. They need to be considered in the context of other risks so that they do not overlap or, exclude each other, while the introduction of a particular measure does not create a new vulnerability.

4.2 Emergency plans and recovery plans

In an enterprise, it is important to think about maintaining the continuity of its activities in the event of accidents. The primary objective of BCM (Business Continuity Management) is to protect property, name and reputation and thus the business owners against financial loss. The deployment of BCM is recommended for both large and small businesses.

The plans developed in the framework of BCM should describe accurately the post-disaster procedures so that the services can be restored to the minimum necessary level in the shortest possible time. Such recovery is only possible if the enterprise in its BCM plan has a scheduled regular and sufficient data backup, ready alternate software, hardware, and personal resources. The plans should include the conditions for starting an emergency plan, order of individual corrective actions, placing alternate resources, personal roles and tasks.

5. Conclusions

In practice, we are confronted with the fact that information security measures are built in a chaotic way as a result of security processes being introduced just as a response following a specific security incident. The individual components of the system then do not bind well together, and the system as a whole is unnecessarily expensive.

Provided that the process of building the information security system is approached systematically in line with a logically drawn up plan, it is possible to achieve a particular balance between the funds spent on security and potential losses resulting from known risks. In the field of research, there is a rule that there is a mutual correlation between security costs and potential damage, and an optimal point of balance.

References

Belás, J.; Korauš, M.; Kombo, F.; Korauš. A. 2016. Electronic banking security and customer satisfaction and in commercial banks, Journal of Security and Sustainability Issues 5(3): 411‑422. DOI: http://dx.doi.org/10.9770/jssi.2016.5.3(9)

Dark, M.J. 2004. Civic responsibility and information security: an information security management, service learning course, nfoSecCD '04 Proceedings of the 1st annual conference on Information security curriculum development, pp. 15-19, Kennesaw, Georgia, ISBN:1-59593-048-5 doi>10.1145/1059524.1059528

Dobrovic, J. Koraus, A. Rajnoha, R. 2018. Activity Management of the Action Plan for a Sustainable Fight Against Tax Fraud and Tax Evasion in Slovakia as Compared With the EU, Marketing and Management of Innovations, Issue 3, pp.313-323, DOI 10.21272/mmi.2018.3-28

Frank, M., Buhman, J.M., Basin, D. 2013. Role Mining with Probabilistic Models, Journal ACM Transactions on Information and System Security, Volume 15 Issue 4, Article No. 15. doi>10.1145/2445566.2445567

Korauš, A.; Kelemen P. 2018. Protection of persons and property in terms of cybersecurity in Economic. Political and Legal Issues of International Relations 2018. Faculty of International Relations of Univerzity of Economics in Bratislava,1. - 2. juni 2018, Virt, Editor: EKONÓM, 2018, ISBN 978-80-225-4506-8, ISSN 2585-9404

Korauš, A., Kelemen, P., Backa, S., Polák, J. 2019. The Challenge of Today's are Cyber Threats In International scientific conference Innovation and Entrepreneurship: Collection of scientific articles. - Ajax Publishing, Montreal, Canada, 25.01.2019. pp. 56 - 61. ISBN 978-1-926711-08-7

Korauš, A.; Dobrovič, J.; Polák, J.; Backa, S. 2019. Security aspects and protection of people in connection with the use of personal identification numbers, Journal of Security and Sustainability Issues, Issues 8(3): 322-335. http://doi.org/10.9770/jssi.2019.8.3(3)

Korauš, A.; Gombár, M.; Kelemen, P.; Backa, S. 2019. Using quantitative methods to identify security and unusual business operations, Entrepreneurship and Sustainability Issues 6(3): 1101-1012. . http://doi.org/10.9770/jesi.2019.6.3(3)

Korauš, A.; Dobrovič, J.; Polák, J.; Kelemen, P. 2019. Security position and detection of unusual business operations from science and research perspective, Entrepreneurship and Sustainability Issues 6(3):1070-1079. http://doi.org/10.9770/jesi.2019.6.3(15)

Korauš, A., Backa, S. 2017. Vývoj kryptomien ako súčasti podnikateľského prostredia. In Sustainability - Environment - Safety 2017. medzinárodná vedecká konferencia. Sustainability - Environment - Safety 2017 : recenzovaný zborník príspevkov zo VII. medzinárodnej vedecekej konferencie konanej 24. novembra 2017 v Bratislave. - Žilina : STRIX, 2017. ISBN 978-80-89753-14-7, s. 203-208.

Korauš, A., Polák, J. 2017. Bitcoin - virtuálny fenomén súčasnosti. In Integrovaná bezpečnosť prostredia 2017. medzinárodná vedecká konferencia. Integrovaná bezpečnosť prostredia 2017 : recenzovaný zborník príspevkov z medzinárodnej vedeckej konferencie konanej 10.novembra 2017 v Rajeckej kotline - Lietavská Svinná. - Žilina : STRIX, 2017. ISBN 978-80-89753-17-8, s. 216-223.

Kritzinger, E., Smith, E. 2008. Information security management: An information security retrieval and awareness model for industry, Journal Computers and Security, olume 27 Issue 5-6, pp. 224-231, Elsevier Advanced Technology Publications Oxford, UK, doi>10.1016/j.cose.2008.05.006

Veselovská, S.; Korauš, A.; Polák, J. 2018. Money Laundering and Legalization of Proceeds of Criminal Activity. In Second International Scientific Conference on Economics and Management - EMAN 2018 , March 22, Ljubljana, Slovenia, Printed by: All in One Print Center, Belgrade, 2018, ISBN 978-86-80194-11-0 https://doi.org/10.31410/EMAN.2018