Dragan Peraković, Ph.D.
E-mail: dragan.perakovic@fpz.hr
Krešimir Šipek, mag.ing.traff.
Tibor Mijo Kuljanić, mag.ing.traff.
University of Zagreb, Faculty of Transport and Traffic Sciences
Vukelićeva 4, 10000 Zagreb, Croatia

IMPLEMENTATION OF CROATIAN INFORMATION SECURITY LEGISLATIVE WITHIN CLASSIFIED ITS

ABSTRACT

Continuous Development of Technology beside the advantages also reveals possible threats for any modern system, first and foremost those which are information or communication dependent. ITS systems in which classified information is handled may become potential target for modern threats (digital data stealing, Denial of Service, etc.) which are especially recognized in cyber space in last ten years. In order to prevent ITS systems to be compromised and abused, it is necessary to provide detailed examination of those systems and implementation of information security measures and standards in all areas of information security that are temporary known. Such process is very complex and appears to be a big challenge because information security is very wide area, legislation and standards are also very complex, and process needs to be continuous. In the scope of this work, it will be shown the approach and the model of adjustment of ITS system with legislation on information security in Republic of Croatia.

***Key words**: Information Security, ITS, Legislation in Republic of Croatia, Security Risk*

1. INTRODUCTION

Constant demands to improve quality of service and growth of requests for various forms of transport have led to development of a new approach to address and resolve traffic problems - Intelligent Transportation Systems (ITS). The development of this approach is particularly noted in the late 20th century, and it has been viewed and analyzed through a number of aspects and analysis. In the scope of mentioned, there are four main benefits of ITS: safety, flow efficiency, Eng. reduction productivity and cost and environment benefits.

Information security is a very broad area that includes a wide range of areas, as well as measures and standards through which is achieved a certain degree of security. Information security is defined as a condition of confidentiality, integrity and availability of data, which is achieved by applying the measures and standards for information security and organizational support for planning, implementation, testing and modifying measures and standards.

2. PREPARATION OF ITS FOR INFORMATION SECURITY MEASUREMENT AND STANDARDS IMPLEMENTATION

In order to prepare ITS for better implementation of information security measures and standards which ITS must meet before classified information of any kind, structured analysis needs to be performed as well as unique model of approach needs to be defined to regulate the ITS in this aspect. Furthermore, as a starting point for implementation of information security for a particular ITS, it is very important to define the highest classification of data which will be handled within ITS.

In development of approach the would arrange ITS within the legal regulations of Republic of Croatia in order to meet measures and standards of information security is important to visualize ITS within the information security with implemented measures that are set by standards (Figure 1).

Figure 1 - ITS-a and information security elements

3. LEGISLATION ON INFORMATION SECURITY IN REPUBLIC OF CROATIA

Legal regulations of the Republic of Croatia that regulates information security are developed within the process of Croatia's accession to international associations, namely NATO and the EU. Through this development, first were implemented legal acts related to information security, namely the Data Secrecy Act (NN, No. 79/07) and the Information Security Act (NN, No. 79/07). Under these laws is uniquely defined the term data as a foundation and starting point that defines the information security measures and standards. This stems from the fact that the data is classified or unclassified and its classification assignment (Figure 2).

Figure 2 - Podatak – ishodište za područja, mjere i standarde informacijske sigurnosti

Furthermore, Information Security Act defines five areas of information security for which information security measures and standards needs to be defined: personnel security, physical security, data security, INFOSEC and business co-operation security (Figure 3).

Figure 3 - Areas of information security

Under the Data Secrecy Act, Information Security Act and the governmental Regulation on information security measures (NN, No. 46/08), a central governmental body responsible for establishing and implementing information security measures and standards in government bodies of Republic of Croatia, the Office of the National Security Council (ONSC), issued five ordinances governing the standards defined for all areas of information security: Ordinance on standards of security checks (March 2011 - a new revision of ordinance, ONSC), Ordinance on standards of physical security (March 2011 - a new revision of ordinance, ONSC), Ordinance on standards of data security (May 2011 - a new revision of ordinance, ONSC), Ordinance on standards of organization and management of information systems security (May 2008, ONSC) and Ordinance on standards for industrial/business co-operation security (May 2008, ONSC).

Closing the legal framework for information security has been further developed because the area of security of information systems is very wide area, which combines elements of all five previously mentioned areas of information security. This stems from the generic definition of an information system - an information system is a system that collects, stores, processes, and delivers the necessary information in ways that are accessible to all members of an organization that wants to use them and have the proper authorization . The central government body responsible for conducting the technical areas of information security within government bodies, the Information Systems Security Bureau (ISSB), issued four ordinances: Ordinance on Standards of information systems security (September 2010 - a new revision of ordinance, ISSB), Ordinance on dealing with cryptography and cryptographic equipment for the protection of classified information (August 2008., ISSB), Ordinance on preventing and responding to computer security incidents (August 2008., ISSB) and Ordinance on security accreditation of information systems (August 2008., ISSB).

4. IMPLEMENTATION MODEL FOR INFORMATION SECURITY MEASURES AND STANDARDS IN ITS

These legal and normative acts are necessary for a systematic and complete implementation of information security measures and standards in complex systems such as ITS. Quality implementation of prescribed information security measures and standards within the ITS depends on segmenting ITS in the parts that coincide with areas of information security. It ensures the proper sequence framework for the implementation of information security measures and standards for a particular area, with the aim of the systematic arrangement of ITS in terms of creating compliant system (Figure 4).

The most important limiting factors in the systematic implementation of information security measures and standards are financial and human resources. Meeting the prescribed information security measures and standards for the handling of classified information that has high classification requires a considerable amount of financial resources. Also, there is a great emphasis on staff that that would carry out its functions under such ITS, because it is also complex and time-consuming to implement security checking process which creates additional financial costs and may cause a time gap between planning and human involvement in implementation (lack of access to classified resources without undergoing safety testing and certification of personnel). Subsequently it can be concluded that the hypothesis "security costs" in most cases is a correct statement.

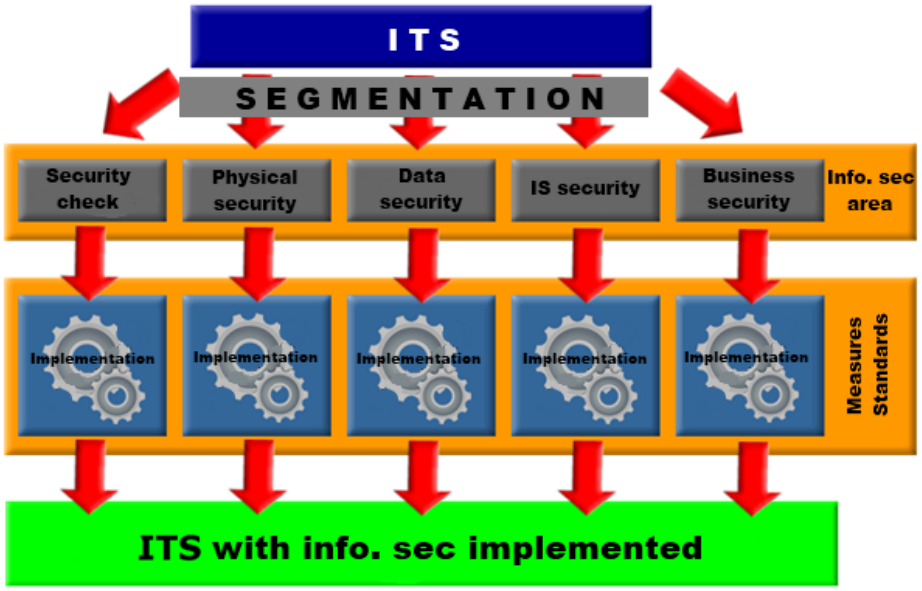

Figure 4 - Model of ITS with implemented information security measures and standards

5. PROCESSES AFTER IMPLEMENTATION OF INFORMATION SECURITY MEASURES AND STANDARDS

To obtain a complete picture of the state of ITS system that went through the process of information security implementation, it is necessary to make the identification and risk assessment after this process. Risk assessment provides a more complete picture and information about the possible solutions to adverse event, despite the implemented information security measures and standards.

Adverse events can affect confidentiality, integrity and availability of information resources in the ITS. Confidentiality refers to the protection of certain content or information

from any intentional or inadvertent disclosure to unauthorized persons. Integrity has to ensure consistency of information and prevent any unauthorized changes to the content. Finally, the concept of availability implies that all relevant information in a reasonable time for that period is available to relevant users. Any of these requirements may be compromised in various ways, either intentional or unintentional human error, either because of flaws and failures of equipment and applications, or for other events.

Risk Management (Eng. Risk Management) is a relatively new discipline in the field of ITS system that resulted from the need of standardization and formalization of procedures related to information security management.

The risk management process is identification of those factors that can adversely affect the confidentiality, integrity and availability of information resources, and their analysis in terms of evaluation of individual resources and the cost of their protection. As a final step of the process is taking appropriate protective measures that would identified security risk take to an acceptable level that is within business objective.

Identification of risks in ITS systems requires a good understanding of the environment in which the system works, and on the other hand, it is necessary to identify all the resources that are important to the organization/company.

Special attention in the framework of risk assessment of ITS systems that are treated with classified information must be given to the first segment of information security, a security check, because it is directly related to the human factor. Specifically, in each system the human factor is the most important of all because it is directly interacting with all other areas of information security. From the standpoint of known metrics that could be applied in assessing the security risks, an individual represents unchangeable variable (each person has a different perception and criteria for any area which is caused primarily by direct and indirect influence of the sociological and the timeframe of events that directly affect a person). Ethics is particularly important factor of a person that is interacting with ITS system, because it directly affects the level of safety evaluation of risk in a particular system.

6. CONCLUSION

Process of implementation of information security measures and standards in ITS is very challenging and dynamic process that must be well and systematically implemented in order to have compliant system. Special attention must be given to the organizational part of the implementation of information security measures and standards, because without the establishment of well-organized implementation process cannot be performed well and standards fully implemented in each area. Moreover, in certain areas of information security organization itself does most of the information security measures and standards (the area of security checking). It should be noted for ITS that went through process of implementing information security measures and standards is not finish, but a continuous process that must follow the dynamics of development of the system and its lifecycle.

LITERATURE

[1] Information Security Act, (Official Gazette, 79/07)
[2] Data Secrecy Act, (Official Gazette, 79/07)
[3] Regulation on information security measures, (Official Gazette, 46/08)
[4] Ordinance on personnel security standards (March 2011. – new revision, ONSC)
[5] Ordinance on physical security standards (March 2011. – new revision, ONSC)
[6] Ordinance on security of information standards (May 2011. – new revision, ONSC)
[7] Ordinance on INFOSEC organization and management standards (May 2008., ONSC)
[8] Ordinance on industrial security standards (May 2008., ONSC)

[9] Ordinance on Standards of information systems security (September 2010. – new revision, ISSB)
[10] Ordinance on dealing with cryptography and cryptographic equipment for the protection of classified information (August 2008., ISSB)
[11] Ordinance on preventing and responding to computer security incidents (August 2008., ISSB)
[12] Ordinance on security accreditation of information systems (August 2008., ISSB)

Internet sources

[13] Main concept of ITS, D.Sc. Ivan Bošnjak, http://www.its-croatia.hr/index.php?option=com_content&view=article&id=145%3Akoristi-i-uinci-its-rjeenja&catid=50%3Alanci-lanova&Itemid=70&lang=hr
[14] Supattra Boonmak, Influence of Human Factors on Information Security Measures Effectiveness under Ethic Issues, Submit to 8th Global Conference on Business & Economics, October 18-19, 2008, Florence, Italy, http://www.mendeley.com/research/influence-human-factors-information-security-measures-effectiveness-under-ethic-issues/
[15] Information system, http://hr.wikipedia.org/wiki/Informacijski_sustavi