THE SECURITY OF INFORMATIONAND MECHANISMS TO ASSURE IT - RESEARCH IN THE BULGARIAN ORGANIZATIONS

Bogdan Țigănoaia, Assist. Prof., PhD, Eng., Politehnica University of Bucharest

Abstract:This paper presents aspects regarding the information security in organizations. There are highlighted, among other, some of the mechanisms used to assure information security in companies. Having as target group the Bulgarian organizations, a pilot research based on a questionnaire regarding the information security and mechanisms to assure it in companies was made. The data are analyzed and the results of this study are presented. Final aspects based on the research findings are also highlighted.

Keywords*: security, information, mechanisms, organization, research*

1. Introduction and theoretical context

Information security is very important as it serves to protect an organization from any threats and risks by ensuring the information is always safe to be accessed, reliable and confidentially protected. In order to ensure information security, organizations normally introduce policies and guidelines which are made available to all members. Despite this effort however, security threats on organizations' information still occur [1]. There are some mechanisms used in organizations in order to assure information security: *digital signature, biometric mechanisms for access control, cryptography of information, steganographic mechanisms* are the most common. There are also *security standards* that are used in order to implement an Information Security Management System. Some words about majority of the solutions above are presented below.

Compared with traditional personal identification techniques such as passwords and PIN codes, *automated biometrics* authentication provides a convenient and reliable method in diverse applications [2].

Cryptography in simple words is an `art or science of protecting data'. The major challenge being faced by it is the intelligence and computational capability of the hacker. All these years the scientists have been working on increasing the computational complexity, but the recent concept of quantum cryptography has added a complete new dimension to this field. The strength of this cryptographic technique comes from the fact that no one can read (`steal') the information without altering its content. This alteration Alerts! the communicators about the possibility of a hacker and thus promising a highly secure data transfer [5].

Security standards from ISO 27k family are the most popular in the field of security assurance:

- ✓ I.S.O. / I.E.C. 27000:2014 – *Information technology – Security techniques – Information security management systems – Overview and vocabulary;*
- ✓ I.S.O. / I.E.C. 27001:2013 - *Information technology – Security techniques - Information security management systems – Requirements;*
- ✓ I.S.O. / I.E.C. 27002:2013 - Information technology – Security techniques – Code of practice for information security controls.

- ✓ Other standards:
  - I.S.O./I.E.C. 27004:2009 – *Information technology -- Security techniques -- Information security management – Measurement;*
  - I.S.O./I.E.C. 27005:2011 – *ISO/IEC 27005:2011 Information technology — Security techniques - Information security risk management;*
  - I.S.O./I.E.C. 27011:2008 – *Information technology -- Security techniques -- Information security management guidelines for telecommunications organizations based on ISO/IEC 27002;*
  - I.S.O./I.E.C. 27010:2012 – *Information technology -- Security techniques -- Information security management for inter-sector and inter-organizational communications;*
- ✓ Other standards under development:
  - I.S.O./I.E.C. 27034-6 – *Information technology -- Security techniques -- Application security -- Part 6: Security guidance for specific applications.*

ISO 27001:2013 can lead to new business opportunities with security-conscious customers; it can improve employee ethics and strengthen the notion of confidentiality throughout the workplace. It also allows the organization to enforce information security and reduce the possible risk of fraud, information loss and disclosure [6]. Any organization, big or small, that holds sensitive information is a candidate for ISO 27001 certification. In particular, companies in the healthcare, finance, public, and IT sectors can benefit greatly from a certified information security management system . An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes processes, people, and IT systems by applying a risk management process [7]. In the next chapter, the results of a study regarding the information security and mechanisms to assure it in the Bulgarian organizations are presented.

2. Research in the Bulgarian organizations

A. Research methodology

Based on a productive cooperation with Prof. Stanimir Stanev from Shumen University, Bulgaria, a pilot research has been conducted. The study, with the target group the organizations from Bulgaria, has as focus point aspects related to the information security and mechanisms used for assure it in the Bulgarian organizations. The main objectives:

- To investigate what mechanisms are used in the Bulgarian organizations for the assurance of information security;
- To study aspects of the information security assurance in Bulgarian organizations regarding: security risks analysis, policies in the field of information protection etc;
- To develop some conclusions, as possible recommendations and changes in Bulgarian organizations, based on the research findings on a topic that is very actual and important for Bulgarian companies: the security of information and mechanisms to assure it.

Variables Measurement

There are two types of variables: nominal scaled and variables regarding the security of information and mechanisms to assure it in Bulgarian organizations. The Table 1 presents, as a summary, the structure of the relevant variables of the study.

Table 1. The map of research variables

Research variables		**Conceptual description**
Nominally Scaled Variables	Demographic Variables	Education, age, gender, professional background – position in the organization etc
		Organizational characteristics: fields of activity, type, number of employees etc
Variables regarding the the security of information and mechanisms to assure it in Bulgarian organizations		The information security risk analysis, policies regarding security and the protection of information, procedures, standards and directives
		Mechanisms used in Bulgarian organizations for information security assurance

The research is based on a questionnaire that includes both opened and closed questions. The qualitative questions are measured using a three point scale (e.g. YES, NO, PARTLY) (adaptation from [3]) and correlative questions are also added for an accurate research and in order to help the respondent for clear and precise answers. The questionnaire, starting with questions for respondents′ demographic characteristics and finishing with questions about the security of information and mechanisms to assure it in Bulgarian organizations, contains topics regarding (selection): organizational characteristics of the Bulgarian companies: type, number of employees, fields of activity etc; the information security risk analysis; policies regarding security and the protection of information; mechanisms used in Bulgarian organizations for information security assurance etc. The questionnaire was distributed to more than 100 respondents / organizations from Bulgaria. The number of daily responses is presented in the Figure 1.

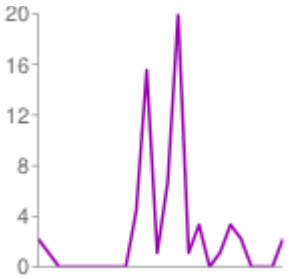


Figure 1: The number of daily responses – study in the Bulgarian organizations

B. Data analysis and research findings

Overall, the structure of the sample in terms of gender was not balanced (according to Figure 2, 78% men and 22% women).

Gender	% of respondents
masculine	78%
feminine	22%

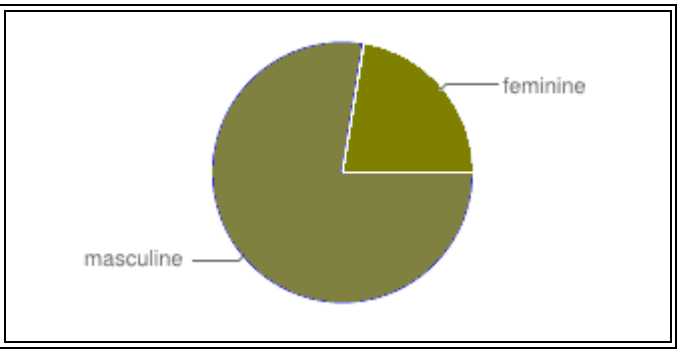


Figure 2: The respondents' gender

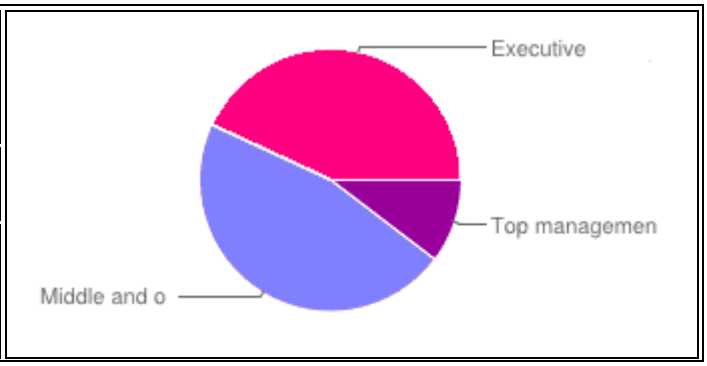
In Table 2 the respondents' age is presented: 33% were of 36-40 years; 26% were of 31 - 35 years; 14% were of 41-45, 12% were of 26-30, only 9% were older than 46 years.

Table 2. The repartition of the respondents' age

Respondents' age	% of respondents
20-25	6%
26 - 30	12%
31 - 35	26%
36 - 40	33%
41 - 45	14%
>46	9%

Most of the respondents have their higher education in the fields of computer science, informatics and economics, but there were respondents with a degree in the fields such as: electronics, veterinary medicine, mechanical and electrical engineering etc. 10% of the respondents have a strategic level managerial function in the organization, 47% operational and middle level management functions. 43% have an executive level position in a Bulgarian organization (no managerial positions - see Figure 3).

Respondents function in a Bulgarian organization	% of respondents
Strategic level	10%
Middle and operational management level	47%



Executive level	43%	

Figure 3: The repartition of the respondents' function in a Bulgarian organization

Table 3 presents the repartition regarding the spheres of activity in the Bulgarian organizations, part of the research: IT, education and research, commerce, financial services, consultancy, national security, civil engineering, telecommunications, e-business, public administration etc.

Table 3. The spheres of activity in Bulgarian organizations which were part of the research

Bulgarian organizations active in	**%**
IT	40%
Education / Training / Research	21%
Commerce	9%
Financial services	7%
Consultancy	5%
National security	3%
Other	15%

According to the Figure 4, the repartition of the number of employees in the Bulgarian organizations part of the study is as follows: 57% have less than 50 employees, only 16% have more than 250 employees, 17% have between 101 and 250 employees and 10% have between 51 and 100 employees.

Number of employees	**%**
≤ 50	57%
51 - 100	10%
101 - 250	17%
> 250	16%

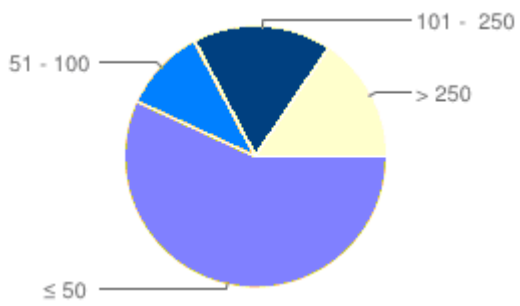


Figure 4: The number of employees in Bulgarian organizations which were part of the study

The Figure 5 shows the repartition regarding the type of the Bulgarian organizations part of the study: 50% are private, 38% are public and 12% are mixed organizations.

Type of the organization	%
Public organization	38%
Private organization	50%
Mixed organization	12%

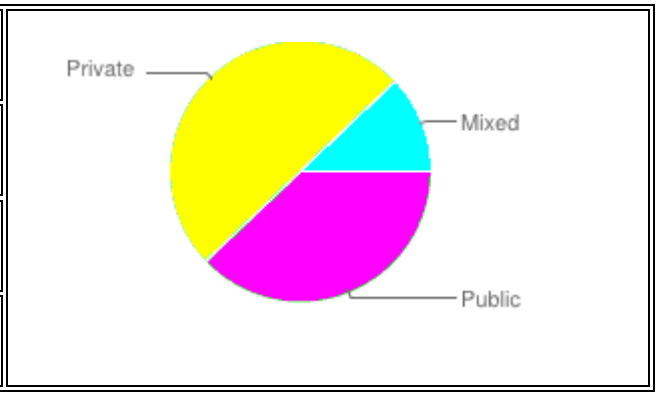


Figure 5: The type of the Bulgarian organizations which were part of the study

Data analysis shows an interesting result in the Bulgarian organizations: 45% of them periodically make the information security risk analysis (which is very important for organizations), 45% of the organizations do not have such a periodical evaluation, but consider that it is necessary (see Figure 6). Only 10% think that a risk analysis is not important and unnecessary.

The Bulgarian organizations periodically make the information security risk analysis	%
Yes	45%
No, I do not think it is necessary	10%
No, but I think it is necessary	45%

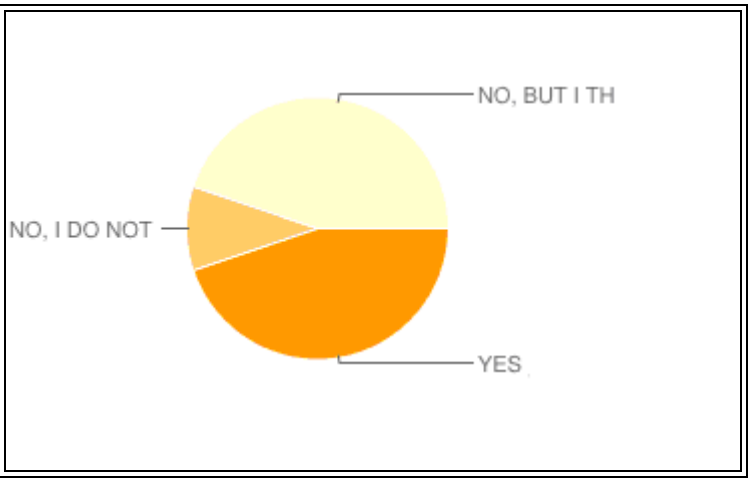


Figure 6: The statistics regarding the security risk analysis in the Bulgarian organizations

The main mechanism used in the Bulgarian organizations to assure information security is digital signature. According to the Figure 7, 76% of the Bulgarian companies use it.Other mechanisms used are: biometric solutions for access control (24%) and cryptography of information (33%). There are no mechanisms to assure information security in 17% (a significant percentage) of the Bulgarian companies. Steganographic solution are not widespread in Bulgarian organizations.

The mechanism	%
Digital signature	76%
Biometric mechanisms for access control	24%
Cryptography of information	33%
Steganographic mechanisms	9%
There are no such mechanisms in the organization	17%
Other	3%

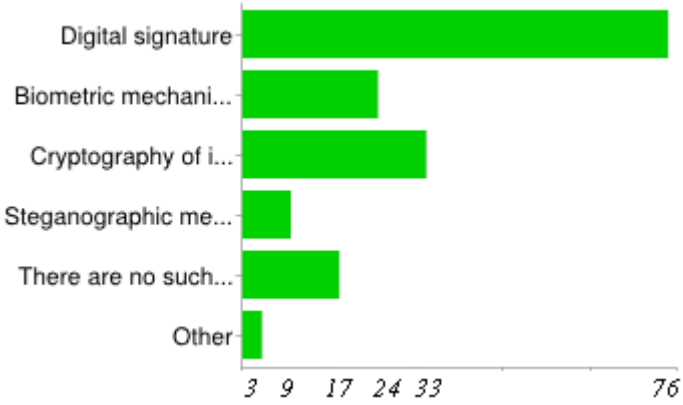


Figure 7: The mechanisms used in the Bulgarian organizations to assure security of information

Other important research findings:

1. At the question: *Is a distinct budget for the security structure / information security assurance in organization?*, the statistics are highlighted in the Figure 8.

The existence of a distinct budget for the security structure / information security assurance in Bulgarian organizations	%
Yes	30%
No, I do not think it is necessary	22%
No, but I think it is necessary	48%

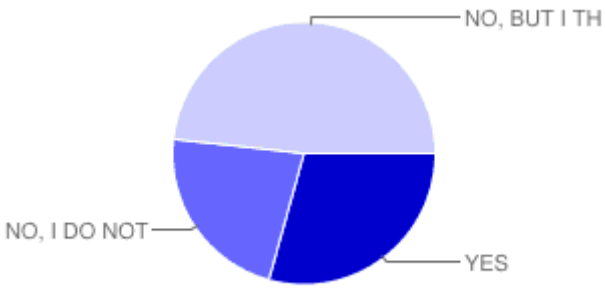


Figure 8: The statistics in the Bulgarian organizations regarding the existence of a distinct budget for the security structure / information security assurance

2. At the question: *Is in the organization a separate security structure (not only guard) responsible for information security of the company?*, the results are presented in the Figure

The existence of a separate security structure (not only guard) responsible for information security in the Bulgarian company?	%
Yes	41%
No, I do not think it is necessary	14%
No, but I think it is necessary	45%

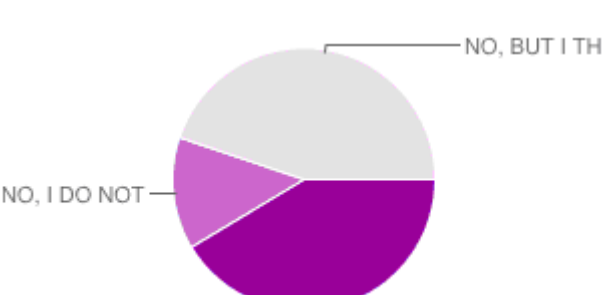


Figure 9: The statistics in the Bulgarian organizations regarding the existence of a separate security structure (not only guard) responsible for information security in the company

3. At the question: *Policies regarding security and the protection of information, procedures, standards and directives exist in the organization and there are disseminated to all employees*, the data analysis reveals the following results (see Figure 10):

The existence of policies, procedures, etc regarding IS and the dissemination to all employees in Bulgarian companies	**%**
Yes	38%
No, I do not think it is necessary	17%
No, but I think it is necessary	45%

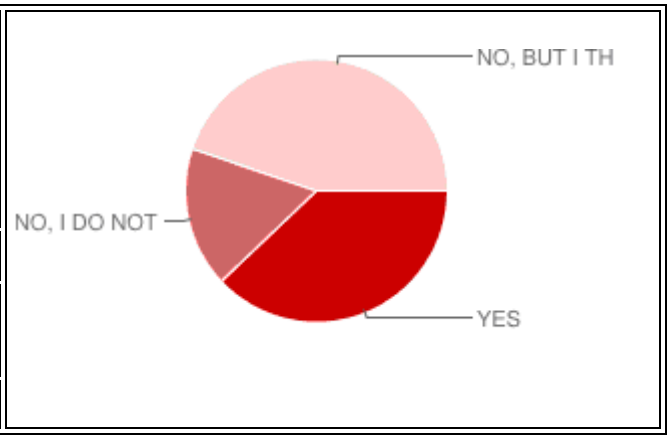


Figure 10: The statistics in the Bulgarian organizations regarding the existence of policies, procedures, etc in the field of information security and the dissemination to all employees

Regarding the annually revision of the policies, procedures, etc in the field of information security, in accordance with the risk analysis, the results are shown in the Figure 11.

The policies, procedures etc regarding IS are annually revised (in accordance with the risk analysis)	**%**
Yes	43%
No, I do not think it is necessary	12%
No, but I think it is necessary	45%

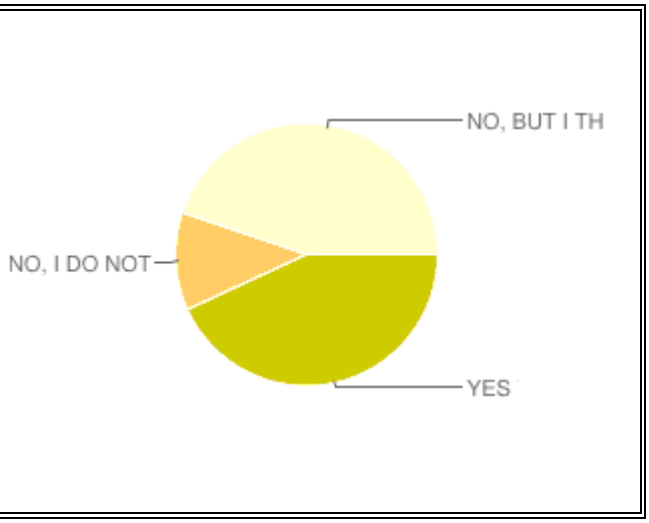


Figure 11: The statistics in the Bulgarian organizations regarding the policies, procedures, etc in the field of information security – annually revision in accordance with the risk analysis

3. Final aspects

According to [4], mostly security managers raise information about technical goals and other controls applied in an ISO 27001 ISMS. This paper tries to outline the importance of information security assurance in organizations and presents a study on this field having as target group the Bulgarian organizations. The results of the study are interesting, as future

work, a comparative analysis regarding the mechanisms used in the Bulgarian vs Romanian organizations to assure information security can be made.

Even though this research has several shortcomings such as sample selection or number of respondents, there are several conclusions:

- The top three mechanisms used in the Bulgarian organizations to assure information security are: digital signature (76%), cryptography of information (33%) and biometric solutions for access control (24%). The last two percentages are still at a low level;
- The information security risks analysis is made only by the 45% of the Bulgarian organizations that were part of the study; the risks analysis is very important for organizations because it helps companies to avoid or reduce losses at any level or type;
- A positive aspect could be the fact that even though 45% of the organizations do not have a periodical risks evaluation, they consider that it is necessary; only 10% think that a risks analysis is not important and unnecessary;
- As a recommendation, organizations should have precise objectives and mechanisms for information security assurance.

Acknowledgements

The work has been funded by the Sectoral Operational Programme Human Resources Development 2007-2013 of the Ministry of European Funds through the Financial Agreement POSDRU/159/1.5/S/132395. I would like to thank Prof. Stanimir Stanev for gathering data and its support in this research.

References

[1]Stambul, M.A.M.; Razali,R., *An assessment model of information security implementation levels*, 2011 International Conference on Electrical Engineering and Informatics (ICEEI), page(s):1-6, 2011.

[2] Shumin Ding; Chunlei Li; Zhoufeng Liu, *Protecting Hidden Transmission of Biometrics Using Authentication Watermarking*, pags 105-108, WASE International Conference on Information Engineering,2010.

[3] Naresh, K. and Birks, D., *Marketing Research. An Applied Approach*, Third European Edition, Prentice Hall, London, 2007.

[4] Humpert-Vrielink, F. , Vrielink, N., *A modern approach on informationsecurity measurement*, 14th Information Security Solutions Europe Conference, ISSE 2012; Brussels; Belgium; 23 October 2012 through 24 October 2012; Code 98644, 2012.

[5] Vignesh, R.S.; Sudharssun, S.; Kumar, K.J.J., *Limitations of Quantum & the Versatility of Classical Cryptography: A Comparative Study*, pags 333-337, ICECS '09. Second International Conference on Environmental and Computer Science, 2009.

[6] http://www.sgs.bg/en/Health-Safety/Quality-Health-Safety-and-Environment/Risk-Assessment-and-Management/Security-Management/ISO-27001-2013-Information-Security-Management-Systems.aspx, accessed in April 2015.
[7] http://www.cert-int.com/services/iso-27001-information-security/, accessed in April 2015.
[8] ISO 27k family of standards (http://www.iso.org/iso/), accessed in 2014.