THE SECURITY OF INFORMATION AND MECHANISMS TO ASSURE IT - RESEARCH IN THE ROMANIAN ORGANIZATIONS

Bogdan Țigănoaia

Assist. Prof., PhD, Polytechnic University of Bucharest

Abstract: The security of information is an important security objective of an organization which assures a good framework to achieve organizational objectives. This paper presents aspects regarding some mechanisms used to assure the security of information in an organization. Regarding this issue, a research based on a questionnaire having as target group the Romanian organizations was made. The results of this study are focus point of the paper. At the end, based on the data analysis, final aspects are presented.

Keywords: security, information, mechanisms, organization, research

1. Introduction and theoretical context

According to the Government of the Hong Kong Special Administrative Region [1], information is an asset to all individuals and businesses. Information Security refers to the protection of these assets in order to achieve C - I – A [1]:

- ***Confidentiality*** - protecting information from being disclosed to unauthorised parties; example in business: sensitive information, such as sales figures or client data, should only be accessed by authorised persons such as senior management and the sales team, and not other operations or departaments;
- ***Integrity*** - protecting information from being changed by unauthorised parties; example in business: important documents or figures should not be changed or altered by unauthorised persons without prior notice;
- ***Availability*** - to the availability of information to authorised parties only when requested; example in business: authorised senior management personnel should be able to access sales figures when needed; or clients should be able to access any of their data kept by the company when they request it;

There are a lot of mechanisms used in organizations in order to assure information security, such as: ***cryptography of information, steganographic mechanisms, digital***

signature, biometric mechanisms for access control. There are also ***security standards*** (some of them presented below) that are used in order to assure information security in an organization or to implement an Information Security Management System.

Security standards – 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** –ISO/IEC 27000:2014 provides the overview of information security management systems (ISMS), and terms and definitions commonly used in the ISMS family of standards. It is applicable to all types and sizes of organization (e.g. commercial enterprises, government agencies, non for profit companies) [2].
- **I.S.O. / I.E.C. 27001:2013 - Information technology – Security techniques - Information security management systems – Requirements** – ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature [2].
- **I.S.O. / I.E.C. 27002:2013 - Information technology – Security techniques – Code of practice for information security controls** – ISO/IEC 27002:2013 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).It is designed to be used by organizations that intend to:
    - select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001;
    - implement commonly accepted information security controls;
    - develop their own information security management guidelines [2].

Other standards:

- **ISO/IEC 27032:2012** - Information technology -- Security techniques -- Guidelines for cyber security;

- **I.S.O./I.E.C. 27008:2011** – Information technology -- Security techniques -- Guidelines for auditors on information security controls;
- **I.S.O./I.E.C. 27033-1:2009** – Information technology -- Security techniques -- Network security -- Part 1: Overview and concepts;
- **I.S.O./I.E.C. 27033–3:2010** – Information technology -- Security techniques -- Network security -- Part 3: Reference networking scenarios -- Threats, design techniques and control issues;

Other standards under development:

- **ISO/IEC 27017** — Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

2. Research in the Romanian organizations

A. Research methodology

This research represents a pilot study which was conducted in order to investigate aspects regarding the security of information and some mechanisms used to assure it in organizations. The target group was consisted of Romanian organizations. In this context, the empirical research in this paper has the following objectives:

- To study what mechanisms are used in Romanian organizations for information security assurance;
- To investigate aspects of the information security assurance in Romanian organizations regarding: security risks analysis, policies in the field of information security etc;
- To develop recommendations (possible changes in organizations) in order to outline the importance of the information security assurance and of the use of some mechanisms in order to assure security of information in companies;

Variables Measurement

There are two types of variables: nominal scaled and variables regarding the security of information and mechanisms to assure it. As a summary, Table 1 shows the structure of relevant variables of the research.

Table 1. The map of research variables

Research variables		**Conceptual description**
Nominally Scaled Variables	Demographic Variables	Gender
		Age
		Professional background
		Organizational characteristics
Variables regarding the security of information and mechanisms to assure it		The information security risk analysis
		Policies regarding security and the protection of information, procedures, standards and directives
		Mechanisms used in Romanian organizations for information security assurance

The qualitative questions were measured using a three point scale (e.g. YES / NO, I DO NOT THINK IT IS NECESSARY, / NO, BUT I THINK IT IS NECESSARY) (adaption from [3]). The respondents express their general opinion regarding the following items (selection): what type of mechanisms for information security assurance are used in the Romanian organizations, aspects regarding the information security risks analysis and policies in the field of information protection in the Romanian companies. The questionnaire includes both opened and closed questions. Correlative items (questions) are also added in order to help the respondent for clear and precise answers.

B. Data analysis and research findings

The questionnaire, starting with questions for respondents′ demographic characteristics and finishing with questions about the security of information and mechanisms to assure it, was distributed to more than 300 respondents, only 174 have filled it. The number of daily responses is shown in the Figure 1.

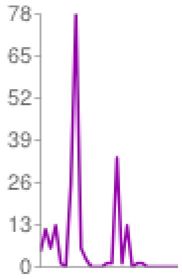


Figure 1: The number of daily responses

Most of the respondents have a technical degree (in computer science), but there were respondents with a university degree in the field of law, public order and national security, management, economics, public administration, banking and finance etc. Overall, the structure of the sample in terms of gender was rather balanced (110 - 63% men and 64 - 37% women). Respondents' age (see Figure 2) was mostly of 20-25 years (70%); 18% were of 26 - 30 years; only 13% were older than 30 years.

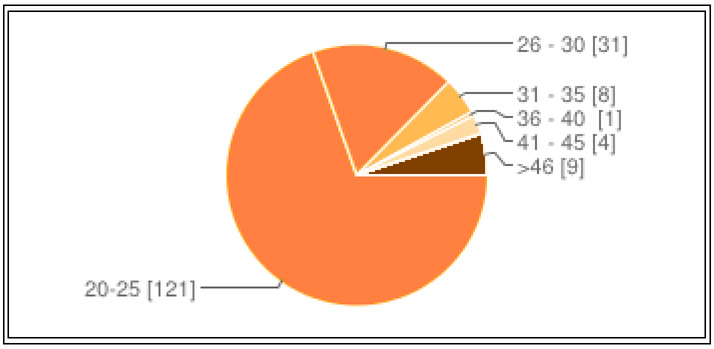


Figure 2: The respondents' age

The repartition of the organizations' (which were part of the research) activity domains can be viewed in the Table 2 and consists of: IT, education and research, national security, public administration, commerce, e-business, civil engineering, telecommunications, financial services, consultancy.

Table 2. The organizations' activity domains

Organizations' activity domains	**% of respondents**
IT	57%
Education / Training / Research	11%
National security	8%
Telecommunications	4%
Other	19%

Regarding the number of the employees in the organizations part of the study, the repartition is shown in the Figure 3 and consists of: organizations with more than 250 employees (50%), 32% less than 50 employees, 7% have between 51 and 100 employees and 11% have between 101 and 250 employees. 44% of the respondents have a middle and operational management position, 5% have a top management position, and 51% are in executive level positions.

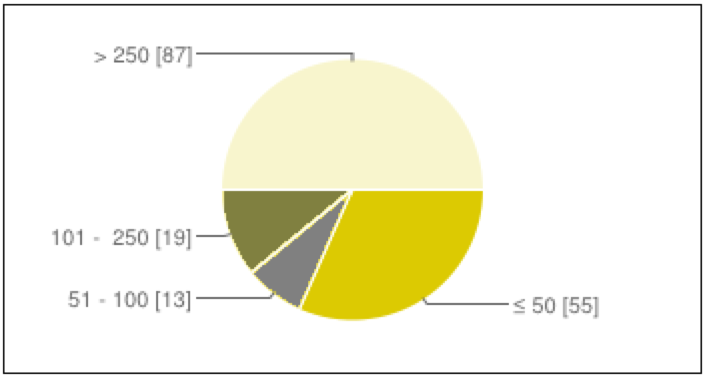


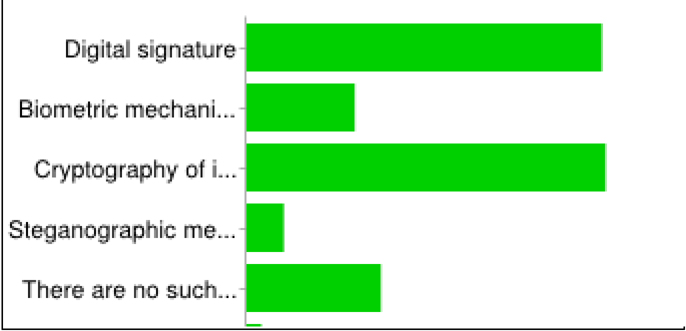
Figure 3: The repartition of the number of employees in organizations part of the study

35% of the organizations part of the research are public, 58% are private and 7% are mixed.

Table 3 The type of the organizations which were part of the research

Type of the organization	**No. of respondents**	**% of respondents**
Public organization	61	35%
Private organization	101	58%
Mixed organization	12	7%

Regarding the mechanisms that are used in the Romanian organizations in order to assure security of information, the statistics can be viewed in the Figure 4.

The mechanism	**No / % of respondents**		
Digital signature	95	55%	
Biometric mechanisms for access control	29	17%	
Cryptography of information	96	55%	

Steganographicmechanisms	10	6%	
There are no such mechanisms in the organization	36	21%	
Other	4	2%	

Figure 4: The mechanisms used in the Romanian organizations to assure security of information

Some research findings can be outlined from that statistics: the main two mechanisms used in the Romanian companies are digital signature and cryptography of information (55%). It is important to mention that there are 21% of the Romanian organizations that were part of the study in which there are no mechanisms to protect information. Also, there are 17% of organizations that use biometric mechanisms for access control and 16% of organizations that use steganographic mechanisms (that are not widespread in Romania). Biometrical access cards, satellite surveillance or closed circuit television camera (CCTV) are among other mechanisms used in Romanian companies.

Data analysis results show that a majority (67%) of organizations periodically makes the information security risk analysis (see Figure 5). This is a very important aspects and research finding because by managing risks (that is one of the pillars that sustain a framework in order an organization to achieve its objectives), the organization can prevent possible losses. 20% of organizations that have not a periodical risk analysis consider that it is necessary such an evaluation. Only 13% think that such an analysis is not necessary for the organization.

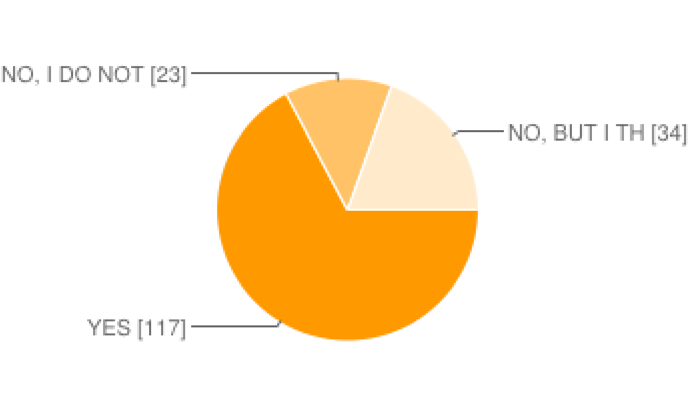
The organization periodically makes the information security risk analysis	**No / % of respondents**		
Yes	117	67%	
No, I do not think it is necessary	23	13%	
No, but I think it is necessary	34	20%	

Figure 5: The statistics regarding the security risk analysis in Romanian organizations

Another finding of the research is that policies regarding security and the protection of information, procedures, standards and directives exist in 72% of the organizations and there are disseminated to all employees (see Figure 6).

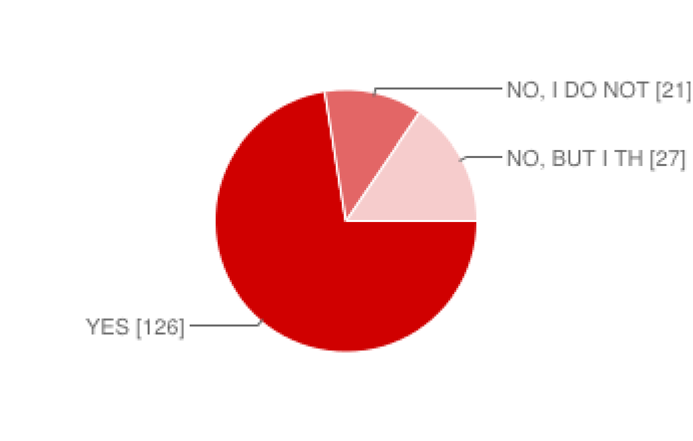
The existence of policies, procedures, etc regarding IS and the dissemination to all employees	**No / % of respondents**		
Yes	126	72%	
No, I do not think it is necessary	21	12%	
No, but I think it is necessary	27	16%	

Figure 6: The statistics in Romanian organizations regarding the existence of policies, procedures, etc in the field of information security and the dissemination to all employees

Policies regarding security and the protection of information, procedures, standards and directives are annually revised (in accordance with the risk analysis) in 68% of the organizations part of the research (see the statistics in Figure 7).

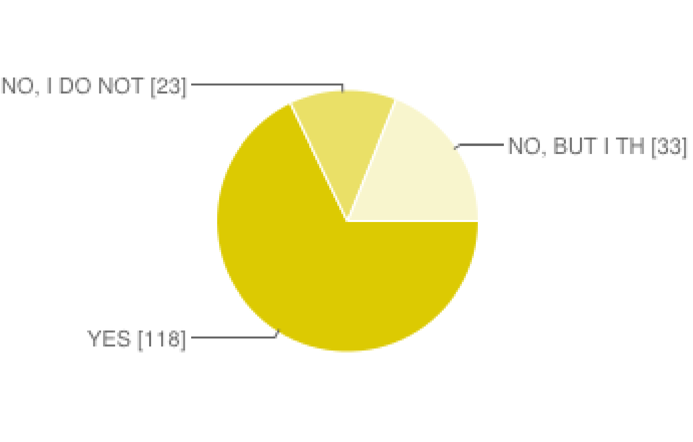
The policies, procedures etc regarding IS are annually revised (in accordance with the risk analysis)	**No / % of respondents**		
Yes	118	68%	
No, I do not think it is necessary	23	13%	
No, but I think it is necessary	33	19%	

Figure 7: The statistics in Romanian organizations regarding the policies, procedures, etc in the field of information security – annually revision in accordance with the risk analysis

Other research findings are presented below:

1. At the question: *Is in the organization a separate security structure (not only guard) responsible for information security of the company?*, the respondents answers are presented in the Figure 8.

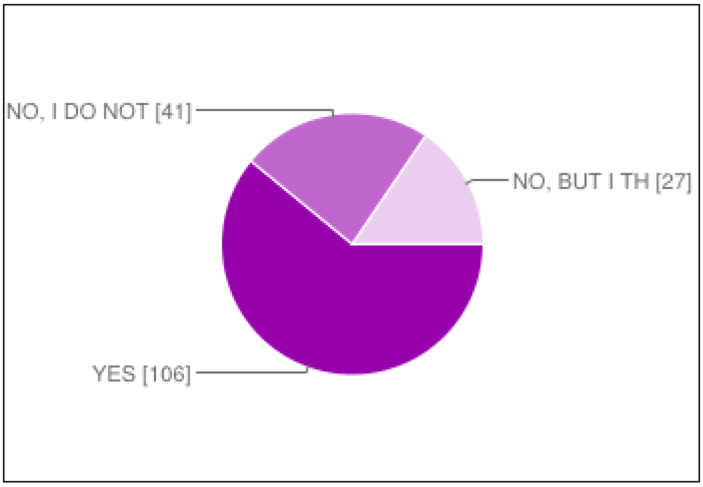
The existence of a separate security structure (not only guard) responsible for information security in the company?	**No / % of respondents**		
Yes	106	61%	
No, I do not think it is necessary	41	24%	
No, but I think it is necessary	27	15%	

Figure 8: The statistics in Romanian organizations regarding the existence of a separate security structure (not only guard) responsible for information security in the company

2. At the question: *Is a distinct budget for the security structure / information security assurance in organization?*, the respondents answers are presented in the Figure 9.

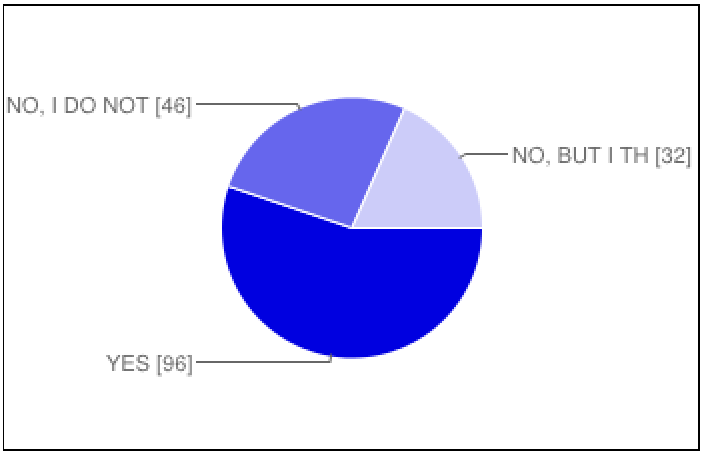
The existence of a distinct budget for the security structure / information security assurance in organization	**No / % of respondents**		
Yes	96	55%	
No, I do not think it is necessary	46	27%	
No, but I think it is necessary	32	18%	

Figure 9: The statistics in Romanian organizations regarding the existence of a distinct budget for the security structure / information security assurance

3. Final aspects

Mostly security managers raise information about technical goals and other controls applied in an ISO 27001 ISMS [4]. According to [5], with ISO 27001:2013 an organization can demonstrate to existing and potential customers, suppliers and shareholders the integrity of the data and systems and the commitment to information security. It can also 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 [5]. This paper tries to outline the importance of all mechanisms used to assure information security in organizations and presents a study on this field having as target group the Romanian organizations. The results of the study are interesting. As future work, a comparative analysis regarding the mechanisms used in the Bulgarian (or other European countries) 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 Romanian organizations to assure information security are: digital signature (55%), cryptography of information (55%) and biometric solutions for access control (17%). The last percentage is still at a low level;
- The information security risks analysis is made only by the 67% of the Romanian organizations that were part of the study; this is still a problem because the risks analysis is crucial for companies: it helps organizations to avoid or reduce losses at any level or type;
- The statistics in Romanian organizations, regarding the existence of a separate security structure (not only guard) responsible for information security in the company, show that only 61% of the companies have such separate structures;
- As a recommendation, organizations should have precise objectives and mechanisms for information security assurance. Another important aspects refers to the security risk assessment and certification of an ISMS according to ISO 27001:2013 – these provide benefits for organizations and reliance for customers.

References

[1] http://www.infosec.gov.hk/english/information/what.html, accessed in November, 2015.

[2] http://www.iso.org, accessed in 2014.

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

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

[5] 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 November, 2015.