An analytical study of information security management in the public sector of Albania.

Grigorina Boce
Department of Information Technology, Mediterranean University of Albania, Tirana, Albania
E-mail address: grigorina.boce@umsh.edu.al

Abstract
Public sector organizations are in the early stages of adopting information security management in Albania. Organizations who have adopted these processes have underestimated information security within the organisation framework. This study specifically investigates the information security management within public sector organizations. Its objective is to organise local organizations with international standards and frameworks in terms of integrating information security management and information technology audits, risks, and control measures. A survey of selected organizations is completed and results are presented in this paper identifying the maturity level of information security management in Albanian organizations.

Keywords: questionnaire, compliance, security awareness.

1. Introduction
Albania is among the countries that are experiencing the rapid development of telecommunications, Internet, and computerization of society. During 2017, the index of internet usage penetration was 66.4% according to Internet World Statistics (Internet World Statistics, 2017). Increased communication constitutes an added value to the economic and social development of a country. At the same time, it exposes the country to the risk of cyber-attacks from state and non-state players. In today's world, given the tendency to permeate boundaries, information security has become a global issue affecting everyone.

Price Waterhouse and Coopers 'reported in The Global State of Information Security 2018 that 29% of businesses have suffered loss or damage of internal records as a result of security breaches, while 30% considered insiders, such as third parties and employees, were the source of these security incidents (Price Waterhouse and Coopers , 2018). [1]

These percentages are higher than those for the previous year. Despite its presence in every business process, information technology (IT) security continues to be treated as a technology issue in many cases, rather than a management issue. Information security management is the process of administering people, policies, and programs with the objective of assuring continuity of operations while maintaining strategic organisement with the organizational mission (Cazemier et al., 2000). Ideally, information security management activities should be driven by organizational objectives to avoid resources being expended on security without the explicit and documented understanding of how it supports the organizational mission (Choobineh, Joobin, Grimaila & Rees, 2007).

However, the increasing use, value, and dependence on computerized systems to support practical operations have increased the importance of incorporating process and organizational issues in security risk management (Drucker, 1999; Blakley et al., 2001).

Information security risk management, the process used to identify the the best protection strategy when forced by a limited security budget, has developed as a required function within organizations that are concerned with their ability to reduce the effects of a breach of information security (Finne, 2000). [2]

It is now widely understood and accepted that information security management and information security professionals can help the organization in achieving its goals and managing responsibillity for privacy and security risks. The aim of this paper is to identify and analyze the maturity level of information security management in Albanian public organizations with the main focus on policies, standards, and employees. The study involves two questionnaires aimed at a sample population of employees listed on IT administrations and results are analyzed to reveal the current status of information security management.

2. Introduction The data regarding information security policies and risk management systems were collected using a standardized questionnaire, involving both a paper-based and a Web-based version, available in the Albanian language. The data collection period was from May 1 to July 30, 2017. The target population was IT directors and IT employees within the IT Administrations of the Albanian government ministries and subordinate institutions. The questionnaire contained nine sections with 52 closed questions in total. From the target group of 250 people, 89 completed questionnaires were received and analyzed in the study. [3]

2.1. Results and Discussion

The questionnaire results showed the information security standards, policies, and employee training used by the organizations. The following are the main findings.

Figure 1 shows that 43.82% of respondents replied that their organization used information security standards. A high percentage indicated that the government lacked actions on these issues with 40.45% and 15.73% of the respondents answering respectively 'No' or 'Not Applicable (N/A)' about the use of standards. [4, 5]

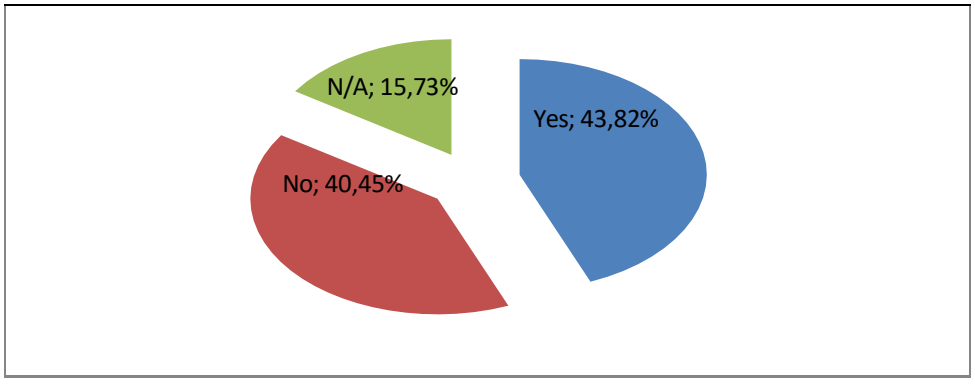

Fig. 1. Application of information security standards
Source: Author

Figure 2 shows 48.31% of employees perceived the information was secure when the company had applied information security standards. Nevertheless, the number of employees that perceived a lack of security, replying 'No' or 'Somehow', was more than a quarter of respondents. There are two possible reasons for these results. First, the company may have failed to effectively apply their information security standards, meaning that not all the employees were aware of the importance of the standards. Second, possibly no person had the responsibility of successfully applying the standards. The second reason is supported by the results shown in Figure 3. [6]

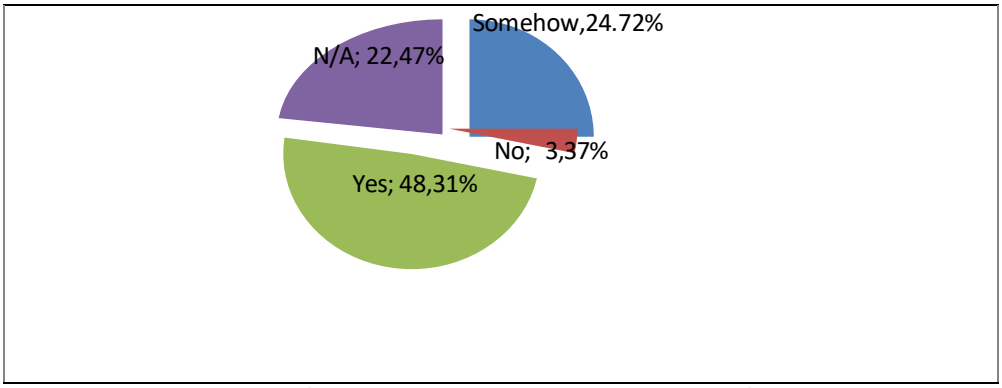

Fig. 2. Employees perception of security when an organization has applied information security standards
Source: Author

Figure 3 shows the results of the question "Is there any employee responsible to ensure that the standards are applied properly?". More than 56% responded 'No' (there were no employees) or 'N/A' (they were not aware of any). [7]

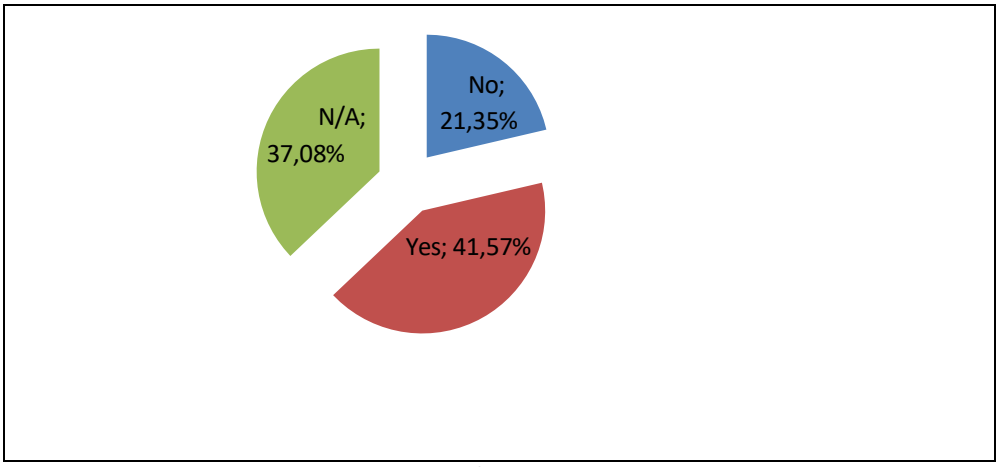

Fig. 3. Employee percentage responsible for ensuring that standards are applied properly
Source: Author

Figure 4 shows that 82% of the employees responded that there was a policy on information security in their organization. [8]

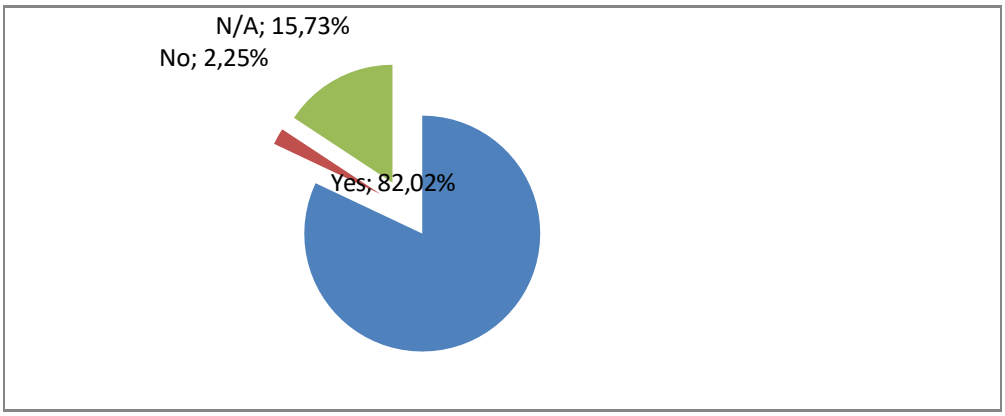

Fig. 4. Information security policy in your organization
Source: Author

Figures 5–7 shows the different responses about the application of the information security policy. Although more than 82% were aware of the existence of a policy (Figure 4), only about 75% recognized that the policy was applied within the company (Figure 5). Figure 6 shows that approximately 53% considered that the policy was revised periodically, while about 70% (Figure 7) responded that the policy was known (and understood) by all employees, which were IT employees within IT directories. [9]

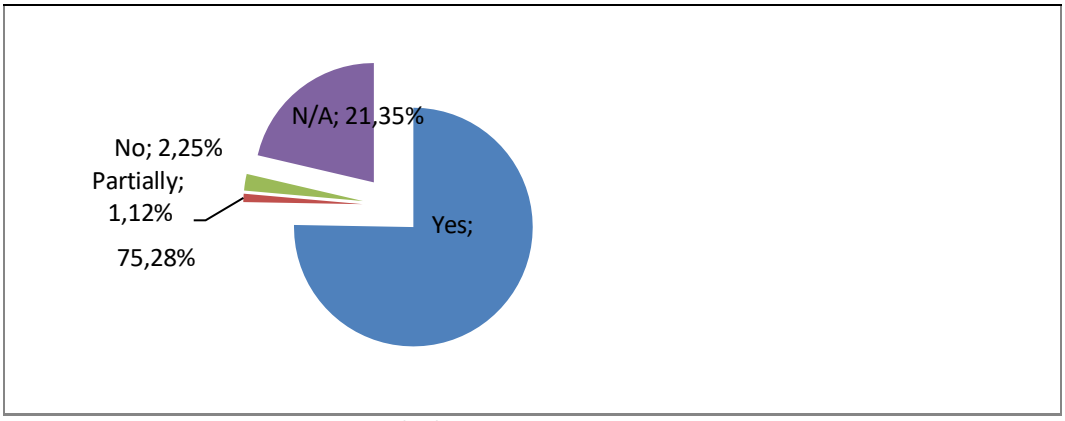

Fig. 5. Application of information security policy in your organization
Source: Author

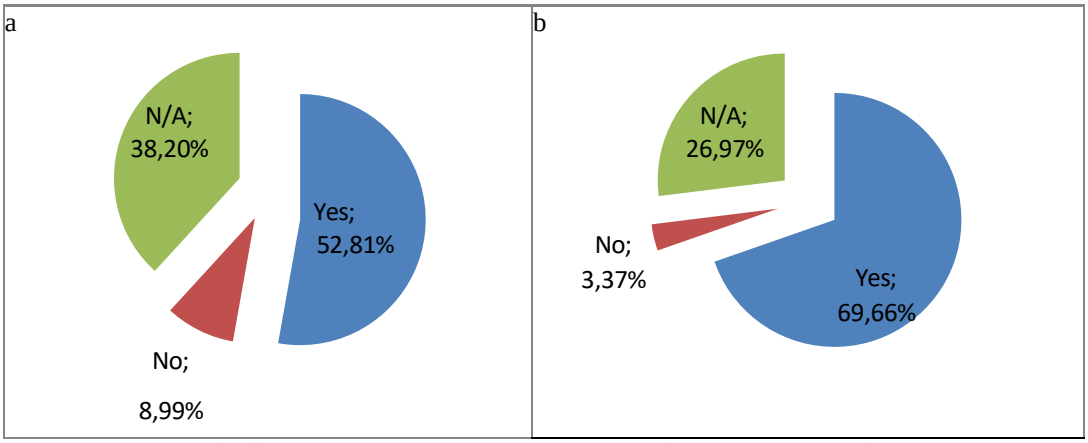

Fig. 6. (a) vision of Information Security policy; (b) knowledge of employees about Information Security policy.
Source: Author

Figure 7 shows the challenges of applying information security standards from the point of view of the employees. The main reason for not applying the standards properly (or at all) was the lack of a budget dedicated to information security (as stated by 37 employees, from 89 responders). The second reason was the lack of qualified human resources in information security (25 employees, from 89 responders).

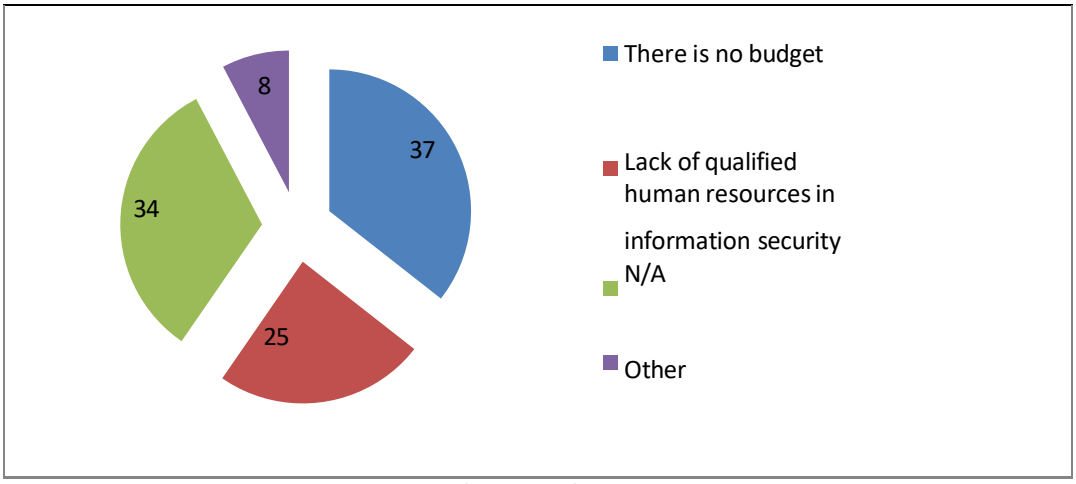

Fig. 7. The challenges of applying information security standards.
Source: Author

Regarding information security policies, the results indicate that more than 80% of respondents were aware of the organization's information security policy, but not all respondents knew whether the policy was revised periodically and whether it was known

to all employees. Hence, the policy did not meet the five criteria of dissemination which are review, comprehension, compliance, and uniform enforcement, considered necessary for enforcing the policy (Whitman& Mattord, 2011). The difference between a policy and a law is that ignorance of a policy is considered an acceptable defense. [10]

According to Nikolakopoulos, (2009), almost 65% of the economic damage caused by information security breaches is due to human error, while only 3% of such is due to malevolent outsiders, based on an assessment of the causes of security breaches. While the use of technology persists as a way of life for the general population, it will continue to affect the way people live, work, and interact with each other. Information security issues may be general occurrences unless appropriate action is taken.

The focus of this paper was to assess information security management in the public sector.

The main findings indicate future work is needed in some areas of information security policies and standards, and with employees. The data reported by IT employees' shows that some organizations do not use information security standards. Thus, the first recommendation is that all organizations adopt a set of information security standards.

Possibly, there is a benefit in using the same set of standards across all establishments.

The second recommendation is that every policy for information security contains attributes that meet the five criteria of dissemination, review, comprehension, compliance, and uniform enforcement. This would facilitate the management of an organizations' responsibillity regarding potential privacy and security breaches. Finally, the results of the questionnaires reveal that a lack of a dedicated budget, and a shortage of trained employees were obstacles in the successful management of information security. Employees would need to receive basic training with optional supplementary training for those seeking to work in particular positions. The final recommendation is that all organizations focus on improving employees' training and aim to reduce potential security breaches.

References

[1] B. Blakely, E. McDermott and D. Geer, "Information Security is Information Risk Management," *Proceedings of the 2001 Workshop on New Security Paradigms,* pp. 97-104, 10-13 September 2001.

[2] J. A. Cazemier, P. L. Overbeek and L. M. Peters, "Security Management (IT Infrastructure Library Series)," *Stationery Office, UK,* 2000.

[3] J. Choobineh, D. Gurpreet, M. R. Grimaila and J. Rees, "Management of Information Security: Challenges and Research Directions",*Communications of the Association for Information Systems:Article 57,* vol. 20, 2007.

[4] P. Drucker, "Management Challenges for the 21st Century," New York, Harper Business Books, 1999.

[5] T. Finne, "Information Systems Risk Management: Key Concepts and Business Processes," *Computers & Security,* no. (19)3, pp. 234-242, 2000.

[6] T. Nikolakopoulos, "Evaluating the human factor in Information Security," 2009.

[7] M. Whitman and H. Mattord, "Principles of Information Security", 4th edition, pp. 91-92, 2011.

[8] "Internet World Statistics," 2018.

[9] "The Global State of Information Security", *Price Waterhouse Coopers,* 2018.

[10] https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html