sciendo

Research Article

Information Security Practices in Public Organizations in Albania

Elda Kuka

Faculty of Economy,
University of Tirana

Prof. Assoc. Dr. Rovena Bahiti

Faculty of Economy,
University of Tirana

Prof. Assoc. Dr. Ezmolda Barolli

Faculty of Economy,
University of Tirana

Doi: 10.2478/mjss-2018-0114

Abstract

Nowadays real time communication is defining and conditioning our everyday life. Increased communication constitutes an added value to economic and social development of the country, but, at the same time, it exposes it to the risk of cyber nature with state and non-state actors. This is the reason why information security has become an important and crucial issue. In this paper we examine Information Security practices among IT departments in public institutions in Albania, using a survey and interviews conducted with IT staff.

Keywords: *information security management, information security practices, information security awareness, questionnaire*

1. Introduction

Due to technological development, information security management has become a very important issue. Although there are numerous technical advances in information sciences, those do not always produce more secure environments (Kuka & Barolli, 2016). Nowadays, information is often referred to as a valuable commodity. This is true in every sector public or private, but it is especially evident in international finance sector as it is involved in processing and transferring valuable information without boundaries (Alarifi et al. 2012; Bandi & Rusell 2004). In this rapidly changing and evolving environment, information as a valuable asset is always under threat. Based on literature, there are more than twelve categories of information threats but we can classify them in three broader categories: the first category of threats include threats that can be classified as accidental or unintentional, such as forces of nature or natural disasters; the second category of threats include deliberate or intentional threats like malware attacks, piracy, hacking, denial of service (DoS) attacks, unauthorized access etc.; the third category of threat include threats that can be classified as contributory or instrumental, such as password issues, equipment failure or failure of backup (Stulz 2003; Afyouni 2006; Easttom 2006). Given the importance of safeguarding organization's sensitive information, after successful threat identification and categorization, every organization should apply effective security controls (United States Government Accountability

Office 2007).

The risk of natural disasters like floods, earthquakes etc., can be mitigated by storing fully operational backup copies of the critical information in remote locations to be used when needed. Human mistakes are the ones that pose information at greater risk. Hackers rely on employees that are careless and, make mistakes like: open every email attachment, use inadequate passwords to protect their computers or accounts, use USB drives which most of the time are infected with malware. Hackers 'attacks evolve and sophisticate very quickly, exploiting system bugs, and employee's distraction or un-satisfaction. The perfect example is ransomware attack on 2017. According to Cybersecurity Ventures, ransomware damages reached $5 billion in 2017. They predict ransomware attacks on healthcare organizations will quadruple by 2020[1].

In this changing environment we should be prepared to stop cyber attacks or, at least to reduce their severity. Organizations more and more are investing in IT infrastructure and IT budget is over 58 percent of the organizational budget and is increasing every year (Byrd & Turner, 2000). But this can't be solely a technical solution that can be handled only by IT department, it should involve every department which processes and handles important information files to make sure that all data protection measures are in place and applied correctly (Purser, 2004).

On the other hand, an information security personnel is necessary to assess, manage and implement information security measures in an organization (Whitman & Mattord, 2012). It is necessary that the organization's approach to information security to be focused on information security management as, information security management protects information from a wide range of threats in order to ensure business continuity (Chang & Ho, 2006).

The aim of this paper is to identify information security practices among Albanian public institutions. More in detail we will analyze some aspects of information security management like: IT budgeting and, information security budgeting; information security policies and information security standards. This paper is organized as follows. On section number two we have described the methodology of this paper, on section number three, we make a general presentation of questionnaires results and interpret them performing a comparative analysis and on section four we describe the conclusions and recommendations.

2. Methodology

For our study, we have used questionnaires about Information Security Policies and Risk Management, created and developed in 2017. The questionnaires were available in printed version and also in Google forms. The target group was IT employees within IT Directorates in Albanian government ministries and subordinate institutions referred herein after as organizations, divided in IT managers and IT staff. The questionnaire contained nine sections. We received 88 responses or completed questionnaires, from the target group of 250 employees. In this paper we will present the results of the questionnaires regarding Information Security practices.

3. Analysis of the Results

As mention before we received 88 completed questionnaires, from the target group of 250 employees in IT units; IT managers and IT staff. The responses were all in printed version although the questionnaire was also available in Google forms. The responses of the questionnaires were later disposed in excel spreadsheets.

3.1 General Information for the organizations

Table no. 1 and table no.2 gives us general information for organizations. Table no.1 shows the results concerning the size of the organization based on the number of the employees. As we can see 55% responded that their organization had more than 101 employees, medium size organization. If we see the results of table no.2 which shows the type of IT unit in the organization,

[1] *https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/*

we can see that 78% responded that the IT unit was directorate. The results show that every organization has IT unit.

Table 1:

Size of your Organization	
1-50 employees	5%
51-100 employees	17%
101-500 employees	55%
more than 1000 employees	24%

Table 2:

The existence of IT unit in organization	
Department	6%
Directorate	78%
Sector	16%

Table no.3 shows the results regarding the existence of specific budget for IT. As we can see 59% of the respondent organizations have specific budget for IT. If we see the results of table no.4, 53% of the respondent organizations didn't have specific budget for Information Security, and 29% didn't have any information if their organization had or no specific budget for Information Security. Surprisingly 29% of the respondents didn't also have any information if their organization had or no specific budget for IT.

Table 3:

Specific budget for IT	
Yes	59%
No	12%
I don't know	29%

Table 4:

Specific budget for Information Security	
Yes	18%
No	53%
I don't know	29%

3.2 Information Security Policies in organization

Table no.5 shows that 82% of the respondents were sure about the existence of information security policy in the organization. Table no.6 shows that 77% of the respondents were sure that information security policy was applied in the organization.

Table 5:

Information security policy existence in organization	
Yes	82%
No	2%
I don't know	16%

Table 6:

The application of information security policy in organization	
Yes	77%
No	5%
I don't know	18%

Table no.7 shows that 93% of the respondents were sure for the existence of backup and data recovery policy. This percentage is slightly higher than the percentage that shows the existence of

information security policy. It means that even though an organization does not have an information security policy, it has data backup and recovery policy, which gives the organization some kind of data protection.

Table 7:

The existence of backup and data recovery policy	
Yes	93%
No	7%

Table no. 8 shows that 80% of the respondents were sure for the existence of the incident response plan.

Table 8:

The existence of an incident response plan	
Yes	80%
No	17%
Not Sure	3%

Table no.9 shows that 94% of the respondents were sure about the existence of procedures for creating and managing user's accounts.

Table 9:

Procedures and regulation in creating and managing users' accounts	
Yes	94%
No	5%
I don't know	1%

Backup and data recovery policy, incident response plan, and procedures in creating and managing accounts are helpful in order to mitigate the risk of cyber attacks.

3.3 Information Security Standards in organization

Table no.3 shows that 43% of the respondents were sure that their organization was applying any standard for information security. Although more than 57% responded "no" or weren't able to give a response. It shows that standards are not implemented properly.

Table 10:

Application of Information Security Standards in organization	
Yes	43%
No	41%
I don't know	16%

Table no.11 shows the feeling of the employees after the application of information security standards. It shows that 51% were not feeling more secure, or were feeling somehow secure or even didn't have any idea. It shows again that the standards are not implemented properly.

Table 11:

Sense of security after the application Information Security Standard	
Yes	49%
No	8%
Somehow	24%
I don't know	19%

Table no.12 shows that only 42% were sure that there was someone responsible for ensuring that

adopted standards are adhered to. 58% were not sure that there was someone responsible or even didn't have an idea.

Table 12:

Employee responsible for proper application of information security standards	
Yes	42%
No	22%
I don't know	36%

The results of table no. 11 and table no.12 show the necessity of trained information security personnel.

4. Conclusions and Recommendations

We examined information security practices among public organizations in Albania. It is important to mention that most of the organizations have IT units and specific budget for IT but they don't have budget for information security. Also, the majority of organizations have information security policies, which help to enforce information security and mitigate the risks. The results are not as good in terms of information security standards. We see that a small number of organizations apply information security standards and the sense of security they offer is low. It shows that these standards have not been applied properly, despite the fact that some of the organizations have someone responsible for ensuring that adopted standards are adhered to. We recommend the application of the same information security standards for all public organizations. This would bring a better application of the standards as well as trained information security employees to do so.

References

Afyouni, H. (2006) "Database Security and Auditing: Protecting Data Integrity and Accessibility", Thomson Course, Canada

Alarifi, A., Tootell, H., Hyland, P., (2012) "A Study of Information Security Awareness and Practices in Saudi Arabia". Paper presented at the The 2nd International Conference on Communications and Information Technology (ICCIT): Digital Information Management, Hammamet

Bandi, F. & Rusell, J. (2004) "Full-information transaction costs" Proceedings of the Conference on Analysis of high-frequency data and market microstructure, Taipei

Byrd, T. & Turner, D. (2000) "Measuring the Flexibility of Information Technology Infrastructure: Explanatory Analysis of a Construct" Journal of Management Information Systems, Vol. 17, no. 1, pp. 167-208/

Chang S.E., Ho C. B. (2006) "Organizational factors to the effectiveness of implementing information security management", Industrial Management and Data Systems Vol. 106, pp. 345-61, 2006

Easttom, C. (2006) "Computer Security Fundamental", Pearson Prentice Hall, USA

Kuka E., Barolli E. (2016) "An overview of human factors in Information Security management in public sector", International Conference Proceedings ISTI-2016

Purser, S. (2004) "A practical guide to managing information security", MA: Artech, Norwood

Stulz, R. (2003) "Risk Management & Derivatives", Mason, Ohio: Thomson South-Western

United States Government Accountability Office (2007) "Information security: Sustained management commitment and oversight are vital to resolving long-standing weaknesses at the Department of Veteran Affairs", Darby, PA: Diane.

Whitman, M. & Mattord, H. 2012 "Principles of information technology", MA: Cengage Learning, Boston