Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 100 (2016) 979 – 986

Procedia Computer Science

Conference on ENTERprise Information Systems / International Conference on Project MANagement / Conference on Health and Social Care Information Systems and Technologies, CENTERIS / ProjMAN / HCist 2016, October 5-7, 2016

Enterprise information systems within the context of information security: a risk assessment for a health organization in Turkey

Şahika Eroğlu[a], Tolga Çakmak[a]*

[a]*Hacettepe University, Department of Information Management, Ankara 06800, Turkey*

Abstract

Enterprise information systems implemented in the organizations are critical assets to provide competitive advantage in changing sectoral conditions and continuity of business processes and management of enterprise resources. In this regard, information security approaches and assessment techniques are used to examine the maturity level of enterprise and determine the risks and potential solutions for enterprise information systems. This study aims to measure information systems in terms of information security and risks. On the other hand, it is also aimed to describe the potential effects of assessment techniques and tools for state organizations to manage their critical assets. In order to achieve these aims, information systems of one of the large scale health sector organizations in Turkey were assessed via an international assessment tool that is adapted to Turkish conditions in some parts like legal regulations. The results obtained through assessment tool provide the current maturity level of the organization and remark the points that should be improved for the security of information systems and the critical components such as risks, processes, people, IT reliance and technology.

Peer-review under responsibility of the organizing committee of CENTERIS 2016

Keywords: Enterprise Information systems; information security; risk assessment

* Corresponding author. Tel.: +90-312-297-82-00; fax: +90-312-299-20-14.
E-mail address: tcakmak@hacettepe.edu.tr

Peer-review under responsibility of the organizing committee of CENTERIS 2016
doi:10.1016/j.procs.2016.09.262

1. Introduction

Information systems, as one of the key business functions for enterprises, support business processes with technological solutions providing cost and time efficiency. They are also used by enterprises to provide competitive advantage, to implement innovations and, to control work flow mostly via electronic environment. As a result of the increasing use of electronic environment in business processes, it is possible to say that there are some potential risks in daily business related transactions as it is in physical approaches. In order to provide security of critical assets, enterprises assess their information systems with some techniques and tools. These assessments also support detections of potential risks and measures to create solutions. According to information security assessments, today, enterprises improve their service quality, increase their values, and efficiently manage business processes. On the other hand, information security contains remarkable components that should be efficiently assessed for all enterprises. Information security assessments and detection of risks are significant factors for preservation of information assets, integrated enterprise management, and sustainability of information systems. As a reflection of system quality, the management of enterprise information security should be carried out carefully [1]. Studies indicate that information systems as one of the critical assets of enterprises and they assessed in terms of security and risk factors. Additionally, the current levels of them and their components should be analyzed by senior decision makers [2].

This study evaluates risks and security applications of a large scale state organization in Turkey serving in the health sector by an international assessment tool also used in different fields (i.e. education and defense sectors). As a case study, the current level of IT reliance, people, processes, risk management applications and technology used for business processes of the health organization in Turkey are measured in the end of the study.

2. Information Security Approaches in Enterprise Information Systems

Many organizations from different sectors use information technologies while performing their business processes. Information systems, from decision-support mechanisms to document management systems, play a vital role for management of work flow among the units of organization. Due to correspondingly changing organizational needs and attempts to provide competitive advantage, organizations were triggered to use of enterprise information systems. Placed in a critical path of organizational structure, information systems have required effective security management issues including risk analysis and assessments. In the light of this information, information security is defined as “the protection of the confidentiality, integrity and availability of information and its critical elements, including the software and hardware that use, store, process and transmit that information through the application of policy, technology, education and awareness [3]” and it is seen as a current research area for organizations for those evaluate information systems in a central position for business processes.

In line with the developments related to information sharing opportunities, it is possible to infer that there is an increase in cybercrime rates. This is also reveals factors that threat business processes and personal information security [4]. In this regard safety issues for enterprise information systems and other critical assets become even more important for almost every sector of business life [5]. Due to the development of technological tools and opportunities and raise of complex structures, and growing threats, information security approaches have emerged for enterprise information systems. It is seen that there are many studies carried out in the literature related to protection and security of information assets and complexity of information systems.

Significantly, in studies conducted on the safety of the enterprise information systems, it is reported that the role of risk assessments and the scope of these assessment should be understood by the IT sector and these assessments should cover all aspects of the IT governance including hardware and software, employee awareness trainings, and business processes [6].

We can possibly say that organizations increasingly become more dependent on technological information systems. Accordingly, they should be more sensitive for the risks and they should use assessment techniques and methods to detect risks and decrease their vulnerability for critical information assets owned by the organization. It's clear that vulnerabilities or errors on information systems leads to serious business crisis and loss of reputation. Therefore, the information security management policies and strategies for organizational information assets become

crucial. Information security policy is the set of rules, standards, practices, and procedures that an organization can employ to maintain a secure IT system [7]. As described in the literature these policies constitute an important part of information security systems for sustainability and protection of organizational information assets. Organizations have many reasons for taking farsighted information security measures. In this context it is stated that there is a need for legal and regulatory studies to protect sensitive or personal data and to motivate organizations for evaluation their critical information assets. According to Johansson, Ekstedt and Johnson [1], there are various risk assessments conducted in IT security and these assessments have different rigor, scope and methods but all of them created for the same aim. That is to identification of risks and decrease their vulnerability to acceptable level for information assets [1].

It is stated that systems for information assets of organizations should be configured in terms of four dimensions. These are technical (hardware and software), physical (media, building, equipment, etc.), organizational (IT alignment, structure, corporate governance, legal, etc.) and managerial (policies, procedures, etc.) aspects [3]. Additionally, it is known that to provide information security management, which defines establishment of the necessary control environment for supporting information integrity, security and availability,

It is seen that different methods and standards [8] were developed in the field of information security and risk assessment. In this context, such internationally accepted standards/rules ISO 27001, ISO 27005, COBIT, PCI, SOX and BASEL II make risk management as mandatory process for organizations.

It is also seen that state organizations and private companies have attempts to provide compliance with TS ISO/IEC 27001 Information Security standard in recent years with the aim of implementing an efficient Information Security Management System. TS ISO/IEC 27001 as a certification for organization with its safe information environment ensures the implementation of information security management system, and guarantee that its use, monitoring, assessments, maintenance and development by the organization in a standardized structure. The most important step to meet such requirements is risk assessments. However, there is not any recommendation about risk assessments techniques in TS ISO/IEC 27001, it is seen as a mandatory application in the standard [9]. One of the most important components of information security studies is risk assessments. It is also confirmed that the risk management with the creation of an information security policy is the first step of the management processes for information security program [10]. Defined as the set of processes to minimize existing risks, risk management involves risk analysis, risk assessments and measurements and evaluation of threats and controls [11] In the light of this information, it is possible to say that identification of risks for the information systems that support to management of enterprise information assets and decrease of their vulnerability to an acceptable level consist the fundamentals of information security approaches. The potential risks and actions can also be determined via risk assessments and they can be analyzed and decisions can be made according to such results.

Risk assessments are also described in many studies and guides published by authority organizations. As one of these guidelines, Guideline for Risk Management for Information Security published by NIST defines risk assessment under the nine steps. These are system characterization, identification of threats and bugs, control analysis, analysis of the threats likely to occur, impact analysis, calculation of risks, control recommendations, documentation of results [12]. On the other hand, another study describes enterprise security risk assessment includes cost justification, productivity, breaking barriers, self-analysis and communication components [6]. In the context of the studies, it is possible to say that risk assessment which is conducted with the aim of providing information security of enterprise systems are not only significant for the system design but also important for organizational security, identity and culture.

Risk management policies and related documents have a vital role for determining, analyzing and following risks in organizations. In this regard, creating awareness and policies related to information security applications for critical assets of organizations are seen important approaches for organizations. Moreover, IT risk fields are also described in the studies. According to one of these studies, IT risk fields involve management and strategy risks, skills and technological development risks, architectural risks business continuity risks, compliance risks, resource risks, support mechanism risks, third party relations, project development risks, change realization risks trust and customer relations, information risks, infrastructure risks and online and web assets [13].

Information security assessments with risk assessments are generally conducted to describe existing security architecture and its recent status. The aim of such studies are defined as evaluation of threats and risks against the information systems and related assets. Assessments certify all implemented applications and acceptable levels of

organizations [14]. Ramachandran states that current status of organizations can be determined by assessments that cover all levels of security architectures including data, application and infrastructure architectures. Similarly, another study reflects that security assessments consists of business impact analysis, threats and vulnerability identification and policy content analysis [15, 16].

Risk management applications are stated as one of the key functions of IT governance and their main function defined as providing a safe environment for business processes. It is also explained that risk management applications and assessments are important tools for well-designed systems and they have effects on the implementation of sustainable and safe environments for business processes as well [14].

3. Methodology

This study aims to evaluate information related functions, systems, and security and privacy issues of a health organization which is one of the large scale organizations in Turkey. Based on the information security assessment definition of U.S. Department of Commerce, National Standards and Technology (NIST), processes, policies, entities, risk management and people were analyzed in the study. In this regard, research questions of the study as follows:

- What is the information security level of the health organization in terms of its critical assets in business processes?
- Which aspects of risk assessment and information security applications are required to improve in the health organization?

In the light of research questions, Information Security Assessment Tool for State Agencies was employed as a research instrument and data collection tool in the study. This tool used and adopted in many fields such as education, defense industry and other state organizations consists of five Likert scale questions (each question has options from 0 to 4) for each section with an explanation area about the responses. Options given in the assessment tool for each question were constructed to describe current situation of the analyzed organization. These options generally are “not implemented”, “planning stages”, “partially implemented”, “close to completion” and “completed”. Beyond the described data collection techniques, interviewing and observation techniques were used to obtain deeper results in the study. According to provided objectives of the study, applications were measured and qualitative and quantitative data were gathered by the assessment tool as a result of the interviews with experts who are responsible for information security and information systems of the health organization. Findings that were reported according to titles given in the assessment tool, revealed the maturity level of health organization.

4. Findings

Findings obtained from the Information Security Assessment Tool for State Agencies are presented in this section. The section titles, such as organizational reliance on IT, risk management, processes, people and technology, were used to report findings and they were categorized according to these titles. Moreover, statements given in the assessment tool were classified by their common attributes and content in some cases. In the end of this section, all categories were evaluated according to scoring tool of the research instrument.

4.1. Organizational Reliance on IT

In the first section of the assessment tool, organizational reliance of the health organization was measured. According to findings, the budget of the organization is in medium level by $100 billion to $1 million. Additionally, the health organization is among the large scale organizations in Turkey with its more than 20 thousand FTE.

Findings indicate that the IT reliance of health organization is in very high level in terms of providing services, value of the information stored in electronic environments, effects of system downtime on operations, organizational change and identity, relations with third parties, new operational processes, sensitivity for information security and privacy issues and political sensitivities. However, IT reliance of the organization is described as high about level of regulations on information security and privacy, and dependency on multi-sided operations by experts.

4.2. Risk Management

Risk management component of the assessment tool provides nine questions to describe information security and privacy issues of the health organization. These questions are classified under the three groups in order to obtain deeper results. These groups are information security and privacy strategy, identification of risks, and monitoring risks and legal framework.

Findings in this section firstly reflect that the current situation of the health organization about having a documented information security and privacy policy and the experts who responded our study marked this question as close to compilation. Furthermore, the content of the information security and privacy policy is also analysed with another Likert scale question. In this regard, this policy partially contains statements related to measuring risks effectively and manage them in an acceptable level. Similarly, it is seen that the policy is in insufficient level about plans related to risk measurement.

The strongest point of the health organization in this section of research instrument is related to risk identification issues. Analysis show that the health organization has conducted risk assessment study in order to describe risks about sensitive assets within two years. It is also understood in the findings that critical assets and related functions, and vulnerabilities and threads were completely described in the organization. Plus, the cost analysis were carried out about the loss of critical assets.

The last part of this section is about the findings related to monitoring risks and legal framework. According to analysis, legal framework related to information security issues was completely followed by the health organization. On the other hand, updates and renovations of information security policy were partially carried out in the organization. It would not be wrong to say that this is an insufficiency such a large scale health sector organization.

4.3. People

The third component of the assessment tools is related to people who work as FTE in the health organization. In this regard, the analysis involve the findings based on the statements about qualifications, roles and responsibilities, trainings, and policies and workflow. The results obtained from the analysis about this part of the assessment tool are displayed at Figure 1.

Analysis indicate that qualifications of people are in medium levels. In this point, it can be described as an opportunity that there are information security experts and staff in the organization. In contrast, low qualifications of employees and lack of authority in these fields are described as remarkable findings for the study. On the other hand, the organization has most of the resources that comply with information security and privacy standards and regulations.

Findings show that almost all responsibilities completely carried out by the organization. It is also seen that only business continuity and disaster recovery plans are in planning stages in the organization.

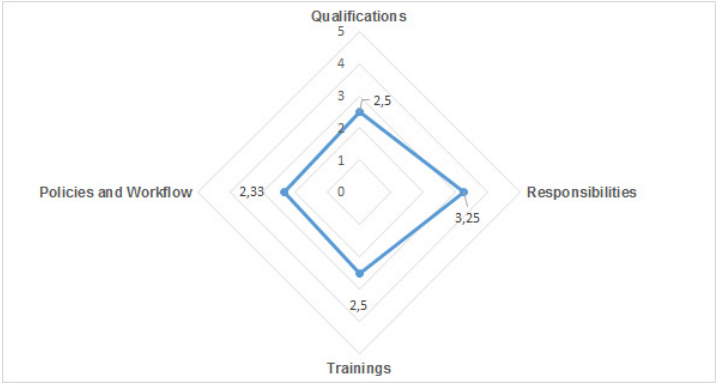

Fig. 1. The role of people in terms of Information Security approaches in health organization

As is displayed in Figure 1, trainings related to information security and privacy should be developed. According to experts, information security and privacy trainings are partially in sustainable structure. However, it can be described as a significant step that information security and privacy trainings are mostly provided in the organization

The weakest point of the organization in this section is related to policies and business processes. Findings reflect that information security units mostly are in collaboration with other units of the organization. Nevertheless, information security units mostly deliver reports to senior management units. It is also evaluated as a disadvantaged situation that business units and senior management policies are in planning stages in the organization.

4.4. Processes

Information security processes were provided under five titles by the assessment tool. These are security technology strategy, policy development and enforcement, information security and procedures, physical security, and security program administration. The mean values for each title obtained from the health organization are displayed in Figure 2.

Fig. 2. Results related to information security processes in health organization

Figure 2 illustrates that the lowest mean value among the information security process components is related to information security policy and procedures. According to findings, some topics are in planning stage for the information policy document. These topics are data transmission, interoperability, log reports and responses, physical security and controls, security reports, investigations on security infringements. On the other hand, responsibilities of employees, use of computer, email, internet and internet policies are partially implemented in the information policy document of the organization. Otherwise, accessibility of personal data, access managements, data classification, storage and disposition issues are mostly described in the information security policy document.

Security program administration issues are also illustrated as lower levels in Figure 2. In this context, the health organization is in planning stages about the renovation of information security and privacy program for all units. Similarly, usage of information security program by every unit independently or periodically is partially implemented in the organization. Furthermore, the health organization is close to complete processes such as inventory of physical and logical network assets, configuration management, reporting security performance values.

Processes and policies about information security and privacy issues are completely tested by the organization.

Findings reveal that processes about updates in security architecture and compliance with new updates are completely carried out by the organization. Management of information security strategy, security processes related to new systems, time management, review and classification processes and documented configuration settings are

mostly completed in the organization. On the other hand, patch management is partially implemented by the organization.

The health organization is in high levels about physical security, policy development and enforcement issues. In this context, procedures related to sharing sensitive information assets within the scope of physical security are partially implemented. It can also be described as a deficiency for the organization that exceptional conditions are partially stated in the policy documents. Furthermore, financial analysis for policy updates, risk identification and privacy issues are almost completed in the organization.

4.5. Technology

The last section of the assessment tool is about technology applications of the health organization. In this context, it is seen that the organization mostly covers technology requirements. Findings show that following issues are completed in the organization:

- Specific protection for domain names and related servers (such as DNS, DHCP)
- Specific protection for remote access services and users
- Protection of web based servers and firewall layers
- Control layers between end tiers
- Periodic scanning of networks, systems and processes for threads and integrity of implementation
- Real time monitoring antiviruses and malwares and abnormal behaviors
- Log records of hardware configuration changes and software configuration and authentication processes

Last but not least, protection of passwords and management, ID validation structures, access management, action reports issues are close to compilation in the health organization. Additionally, it is seen that session management, antivirus management, updates and patches for operating systems should be improved in the light of findings.

4.6. General Overview

In addition to specific findings detailed previous sections of the study, the health organization analyzed in terms of general overview. In this regard, the general overview of components is summarized in Figure 3.

According to findings presented in Figure 3, IT reliance of the health organization is higher than other components. Plus, risk management and technology applications (80.5% ve 79.4%) are other high level components of the organization. Processes and people (67.6% and %59.6%) are the lowest components of the organization in terms of information security and privacy assessment.

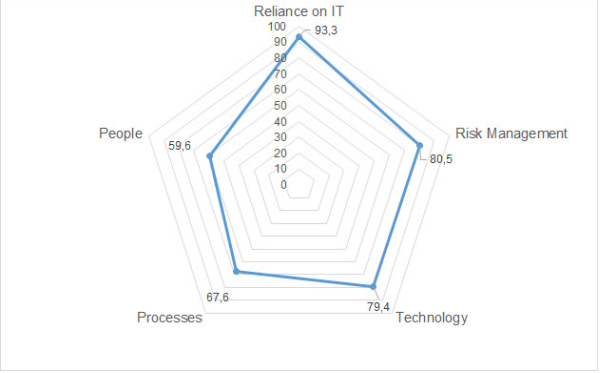

Fig. 3. General overview of information security components.

As a result of the points obtained from the assessment tool, the score of the health organization was calculated as 233 points. According to assessment tool, the health organization is in good level and its IT reliance is in very high level.

5. Conclusion

Threats that are mainly based on the bugs in information systems negatively affect business processes and also organizational identity and culture. They can also cause to loss of organizational values and their service quality. Organizations use risk assessment techniques in order to identify existing and potential risks, decrease their vulnerabilities and providing secure environments for information assets. Results obtained from risk assessments enlighten the current maturity levels of organizations and they also support the decision making processes to manage risks in an acceptable level for units. Risk assessments can also be stated as a guide for increasing productivity and sustainability of information systems. As a result of the risk assessment study conducted in Turkish health organization following results were obtained in the study:

- The health organization is located in large scale state agencies and its organizational reliance on IT is in very high level. In this context it is seen that important part of business processes is carried out via electronic environment.
- High dependence of the organization on technology also requires having the opportunities related to usage of high technology. In this context the technologic capability of the organization is in highest levels among the other components.
- It is understood that the factors which the organization is in weak levels are related to people who is used the systems. At this point the organization significantly needs to applications and trainings supporting to improve staff competencies
- In terms of procedures, it's understood that the organization needs to improve its information security policy in the sense of content. From this point of view organizational policy document should be developed by covering technical specifications and exceptional conditions.

Lastly, in addition to above mentioned conditions, the health organization is in “Good” level according to scoring section of the assessment tool. It is also seen in the results that the organization is in strong levels in terms of infrastructure and technical attributes of information systems. However, components related to management of information systems, such as people, policies and procedures should be improved by new regulations and decisions to increase efficiency of business processes.

References

1. Johansson E, Ekstedt M, Johnson P. Assessment of enterprise information security : The importance of information search cost. *Proceedings of the Annual Hawaii International Conference on System Sciences* 2006; 9: **219.**
2. Ekstedt M, Johnson P, Lindström A, Gammelgård M, Johansson E, Plazaola L, Silva E, Lilieskӧld J. Consistent enterprise software system architecture for the CIO: A utility cost approach. *Proceedings of the 37th annual Hawaii International Conference on System Sciences (HICSS)* 2004.
3. Khoo B, Harris P, Hartman S. Information security governance of enterprise information systems: an approach to legislative compliant. *International Journal of Management & Information Systems* 2010;**14**:3.
4. Henkoğlu T, Yılmaz B. İnternet erişim özgürlüğünün kısıtlanması: Türkiye üzerine bir değerlendirme (Restrictions of internet access freedom: An evaluation study of Turkey). *Bilgi Dünyası* 2013;**14**: 215-239.
5. Ross R. Managing enterprise risk in today’s world of sophisticated threats :A framework for developing broad-based, cost-effective information security programs. *The EDP Audit, Control nd Security Newsletter* 2007; **35**:1-10.
6. Schnittling R, Munn A. Performing a Security Risk Assessment. *Isaca Journal* 2010;1.
7. Kadam AW. Information security policy development and implementation. *Information Systems Security* 2007;**16**: 246–256.
8. Moulton R, Coles RS. Applying information security governance. *Computer Fraud & Security* 2003; **22**: 580-584.
9. TS ISO/IEC 27001. *Bilgi teknolojisi – Güvenlik teknikleri - Bilgi güvenliği yönetim sistemleri – Gereksinimler*; 2006.
10. Takçı H, Akyüz T, Uğur A, Karabağ R, Aktaş FÖ, Soğukpınar İ. Bilgi güvenliği yönetiminde risk değerlendirmesi için bir model. *Türkiye Bilişim Vakfı (TBV) Dergi* 2010; **3**.
11. Şahinaslan E, Kandemir R, Kantürk A. Bilgi güvenliği risk yönetim metodolojileri ve uygulamaları üzerine inceleme”, *ABGS 2010 – Ağ ve Bilgi Güvenliği Sempozyumu*. Ankara: EMO; 2010.
12. National Institute of Standards and Technology (NIST). *Risk management guide for information technology systems*. Special Publication 800-830: 2001.
13. Bağcı B. *Bilgi Teknolojileri Risk Yönetimine Genel Bakış*. *Member of Deloitte Touche Tohmatsu 2012*: 1-11
14. Ramachandran, Jay. Designing Security Architecture Solutions. New York: Wiley; 2002.
15. King CM, Dalton CE, Osmanoglu TE. *Security Architecture: Design, Deployment & Operations*. New York: Osborne/McGraw-Hill; 2001.
16. Farah G. *Information systems security architecture a novel approach to layered protection a case study: GSEC practical version 1.4b*. Sans Institute; 2005.