Evaluation of Information Security Approaches: A Defense Industry Organization Case

Tolga Çakmak[1], and Şahika Eroğlu[1]

[1] Hacettepe University, Department of Information Management, Ankara, Turkey
{tcakmak, sahikaeroglu}@hacettepe.edu.tr

Abstract. Information security systems are important to ensure the business continuity and protect organizations against the potential risks. In this context organizations have to analyze their information system processes and they should develop their information systems according to results of the analysis. This paper aimed to analyze information security approaches in a defense industry organization in Turkey via an assessment tool that is widely used by organizations for their information security analysis. The results obtained from assessment tool provide an insight about information security level and observe the current situation of information security processes and infer approaches that are necessary to develop for the defense industry organization.

Keywords: Information security, knowledge management, information security assessment.

1 Introduction

Organizations are one of the most efficient factors for the development of communities. They generally interact with their internal and external environments. As a result of this interaction, they can create not only services or a particular product required by target group but also they create continual information and information resources especially in electronic environments. In this respect, it would not be wrong to say that knowledge management is a key point for organizational development with the convergence of new technologies. Besides knowledge management provides management of information created for organizational goals, organizational effectiveness and productivity, and competitive advantage.

Advancements in Internet and web technologies, new perspectives for competitive advantage and changes in administrative approaches increase the importance of knowledge management for organizations. Especially in the 1990's with the use of information systems in modern sense, knowledge management and security issues have become a vital factor for organizational development and competitive advantage in a global world. Many standards, policies, regulations, information security assessment methodologies and assessment tools were developed for organizations. In this respect, organizations can implement information security approaches according to standards and revise their information security approaches in accordance with

assessment tools and they can also take countermeasures against determined risks as well.

In the light of the information mentioned above, this study evaluates information security level of a defense industry organization where ISO 27001 Information Security Standard has been fully implemented and information security approaches mainly used due to the nature of the organization.

2 Information Security and Developments in Turkey

Information security is one of the most important components for many organizations who achieve their organizational goals via information technologies and information systems. Blackley, McDernott and Geer [1] express that the emergence of new risks dealing with technological developments has a huge effect on organizational approaches about information security. Authors also indicate that risk assessments for information systems should be carried out by organizations. As many researchers, governmental organizations and their reports have demonstrated, organizations principally should evaluate and assess their information security applications, approaches and determine organizational risks.

There are many definitions about information security in the field of organizational knowledge management and library and information science One of these definitions emphasized that “information security is a collective efforts that are made for security of information processing, protection for unauthorized access, long term preservation, migration, emulation and storage of data/information in electronic environments” [2]. Furthermore, it is inferred that information security is not only a term about technology but it is also about organizational identity. Studies in this topic asserted that information security is important for all work processes such as creation, processing and storage of information as well as information in information systems and information systems [3][4].

The term of Information security was mentioned and described in Turkey for the first time in 2005 with the publication of "e-Transformation Turkey Project Principles of Interoperability Guide" [5]. The Guide identifies the main aims of information security as protection of information processed via information life cycle (in capture, creation, usage, storage, transmission and destruction phases) within the organizations and providing the privacy, integrity and accessibility of information transmitted between the organizations. Security and privacy of personal information was also considered as one of the main themes in “Information Society Strategy Action Plan (2006-2010)” that was published by Ministry of Development. Some important points covered in the plan are listed below:

- requirement for establishment of Information Systems Disaster Recovery Management Center,
- preservation of information related to national security in electronic environments,
- regulations about legal infrastructure for development of information security systems [6].

Some researches on the information security approaches were also conducted in Turkey by private companies. According to one of these researches, (Ernst & Young Company) 73% of organizations makes investments for information security and 50% of organizations use information security standards and 30% of organizations don't have a connection between their risk management and information security units. Research results also revealed that the information security is perceived as a technological issue by Turkish companies [7].

3 Research Design

In the light of increasing importance of information security approaches in organizations, this study focused on identifying the information security approaches of a defense industry organization in Turkey. Case study methodology was used to achieve research objectives. As quoted from Thomas [8] case study methodology is "analyses of persons, events, decisions, periods, projects, policies, institutions, or other systems that are studied holistically by one or more methods". In addition to Thomas's definition, Zainal [9] alleges that a limited number of events, conditions and relationships of real-life phenomenon can be explored and investigated via case study methodology.

In this context, the research covered by this paper particularly demonstrates the current information security approaches and explores information security requirements in the defense industry organization according to main objectives listed below:

- to provide an insight about information security standards and approaches that are widely used in recent years by several organizations in Turkey,
- to provide a sample assessment for information security approaches,
- to give point to importance of information security implementation within the organizations.

4 Data Collection and Research Instrument

Information security assessment is defined by U.S. Department of Commerce, National Standards and Technology (NIST) in 2008 in a publication titled as Technical Guide to Information Security Testing and Assessment [10]. NIST defines Information Security Assessment as: "the process of determining how effectively an entity being assessed (e.g., host, system, network, procedure, person - known as the assessment object) meets specific security objectives". NIST also directs organizations for the information security assessments by providing descriptions of the information security assessment methods. In this regard, three assessment methods -testing, examining and interviewing- can be used for information security assessments according to NIST [10]. In this respect, examining which is defined by NIST as: "the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve

clarification, or obtain evidence" and interviewing methods were used to gather data about information security approaches in the defense industry organization.

In parallel with research design and objectives of the study, data gathered via an assessment tool and structured individual interviews with information security experts who work in the defense industry organization. In order to get deep knowledge for the research objectives legal regulations, assessment tools, and information security standards were reviewed. As a result of the reviews, Information Security Assessment Tool for State Agencies, derived from Information Security Governance Assessment Tool for Higher Education which was developed by EDUCAUSE in 2004 to support U.S. National Cyber Security Partnership Corporate Governance Task Force Information Security Government recommendations, was chosen for analysis.

Information Security Assessment Tool for State Agencies was developed with the aim of evaluation of the people, process, and technology components of cyber security [11]. It is also expressed that this tool is a pointer for organizations in terms of the maturity of their information security program. The sections in this tool can be divided into two main parts consisting of reliance of information technology and the maturity of information security governance.

5 Data Analysis

Qualitative and quantitative findings obtained via the assessment tool were analyzed according to scoring section of the tool. The data that were gathered via tool created a score which demonstrates information security level of organization about organizational reliance on information technology, people, risk management, processes and technology. Scores obtained in these sections were reported and evaluated to reflect current situation and needs of defense industry organization.

6 Results

In this section of the study, results obtained from the assessment tool, Information Security Assessment Tool for State Agencies, are presented. In parallel with the research objectives, assessment tool provides overall assessment and considers current situation, requirements and improvements for the defense industry organization. In this context, assessment tool indicates the results of main components of information security like organizational reliance on IT, risk management, people, processes, technology and general overview.

6.1 Organizational Reliance on IT

In the beginning of the assessment, general structure of the test-bed and organizational reliance on IT of the defense industry organization were identified by the first section of the assessment tool. According to results, annual budget of the

organization (between $100 million to $1 billion) is in medium level. Results also reflect that the defense industry organization is in very low level with its number of employees (less than 500 employees).

Organizational reliance on IT and general characteristics of the test-bed were investigated via 13 likert scale questions. According to the answers given to this part of the tool, the defense industry organization is in high level in terms of dependence upon information technology systems, the internet to offer services to customers, outreach programs, conduct research, and support services. Approaches about the value of organization's intellectual property stored and transmitted in electronic form is in medium level. Information security experts thought the impact of major system downtime on operations is in medium level for the organization as well.

According to results, degree of change within the organization, impact to organization's operations from an internet outage, dependency on multi-site operations, and plans for multi-site operations (i.e. outsourced business functions, multiple locations and new collaborations) are in low level. Information security experts also noted that the organization is in very low level in terms of potential impact to national or critical infrastructure in case of outage, interruption, or compromise to systems. It is also expressed that sensitivity of stakeholders and customers for security and privacy, and extend of operations dependent upon third parties are in high level. Furthermore, it was determined that organization's level of regulation regarding security and privacy is in mid-level.

Lastly, potential impacts on reputation of security incidents (i.e. negative press and political pressure) are in low level for the organization according to information security experts. It is also stated that the organization have low business programs in a politically sensitive area that may make it a target of a violent physical or cyber attack from any groups.

6.2 Risk Management

Information security experts were asked to describe risk management approaches of the organization via nine questions provided by the second part of the assessment tool. Risk management approaches are one of the main functions of the organizations in the defense industry. Results revealed that whole of the risk management metrics directed by the assessment tool are fully implemented. These can be listed as follows:

- Information security and privacy program were fully documented,
- Risk assessments to identify key objectives that need to be supported by the information security and privacy program were conducted within the last two years,
- Critical assets and relevant business functions were fully identified,
- Information security threats and vulnerabilities associated with each of the critical assets and functions were fully identified,
- Costs and cost analysis for the loss of each critical asset or function were carried out,
- A written information security strategy that seeks to cost-effectively measure risk and specify actions to manage risk at an acceptable level with minimal business disruptions was developed,

- Information security strategy of the organization fully includes plans that seek to cost effectively reduce the risks to acceptable level,
- Information security strategy of the organization is reviewed and updated at least annually or more frequently when significant business changes require it,
- Processes to monitor federal or state legislation or regulations and determine their applicability to the organization were fully implemented.

6.3 People

Another section of the assessment tool within the scope of information security approaches is assessment of people in the organization. In this regard, the analyses involve the answers given to questions about responsibilities, management, information security functions, and education and training program. The results obtained from the analyses about this part of the assessment tool are displayed at Figure 1.

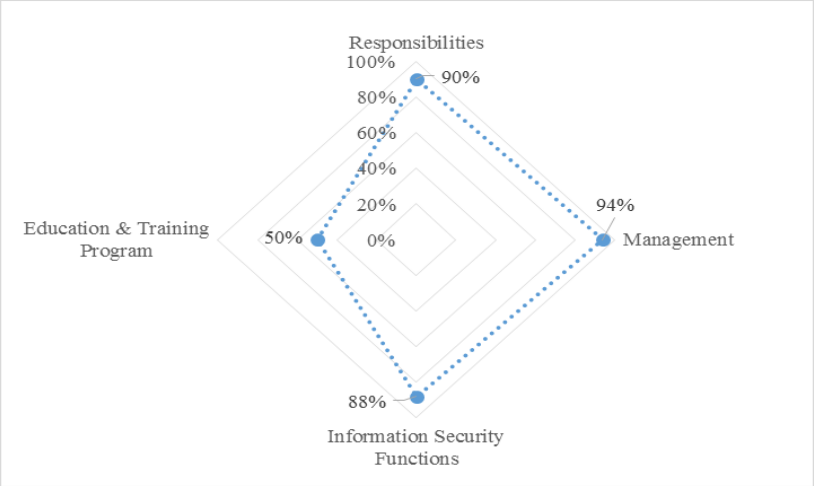

Fig. 1. Information Security approaches in terms of people in defense industry organization

According to the results in Figure 1, the organization meets the most of the requirements about responsibilities (90%), management (94%) and information security functions (88%). However, it was found that half of the education and training program requirements can be met with existing information security approaches of the organization.

According to the results demonstrated in Figure 1, Information security experts stated that only some units have employees for liaising with business units to identify any new security requirements based on the changes to the operations. It is also expressed that most of the business unit managers and senior managers have specific programs in place to comply with information security and privacy policies and standards. Furthermore, results reflect that most of the information security functions were actively engaged with other critical functions such as IT, Human Resources, etc. On the other hand, education and training program requirements about information security and privacy issues were partially implemented by the organization.

6.4 Processes

Analyses on information security processes were considered under five titles by the assessment tool. These titles are security technology strategy, policy development and enforcement, information security and procedures, physical security, and security program administration. In this context, the ratings related to the information security processes in the defense industry organization are displayed in Figure 2.

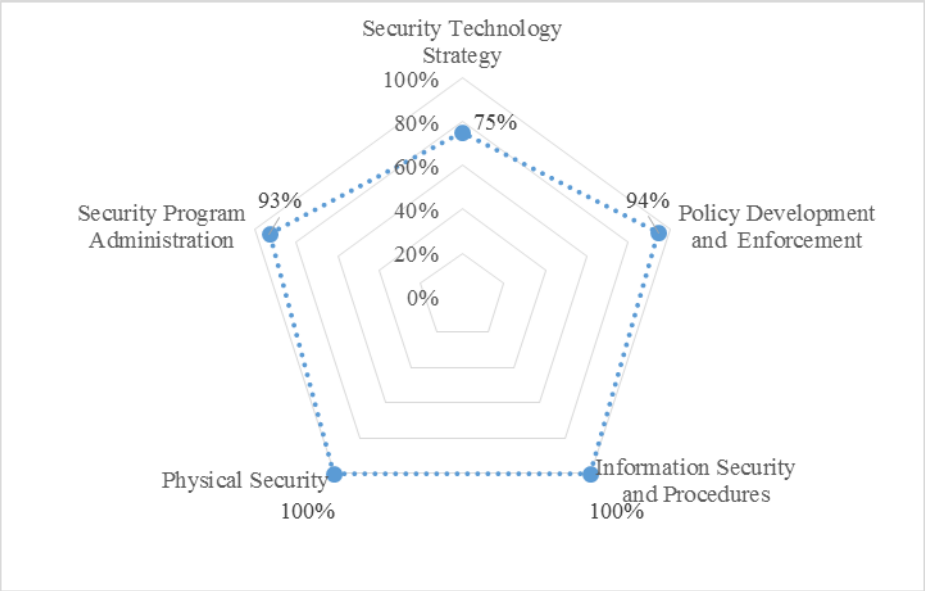

Fig. 2. Information Security Processes in Defense Industry Organization

As it can be seen in Figure 2, the organization has fully implemented processes about information security and procedures, and physical security processes. On the other hand, existing processes can only meet 75% of the requirements about security technology strategy. It is also considered that most of the requirements about security program administration (93%) and policy development and enforcement (94%) are covered by the organization. Assessment tool also reveals that the organization is close to completion of following required processes in terms of security technology strategy:

- Periodically updates on security technology strategy,
- Review of existing systems,
- Processes and procedures involving the security personnel in evaluating and addressing any security impacts before the purchase or introduction of new systems,
- Identification of work processes for incompatible systems in terms of information security,
- Implementation of specific, documented, security related configuration settings for all systems and applications,
- Developments for patch management strategy, policy and procedures.

Assessment tool also reflects that periodically evaluation of information security and privacy program, and practices for each business unit is not fully implemented by

the organization. Additionally, analysis on political development and updates are close to completion in the organization.

6.4 Technology

Technology as one of the key information security components was also investigated within the scope of the study. Results indicate that almost every requirement is fully implemented by the organization. These requirements can be listed as follows:

- Protection of internet-accessible servers by more than one security layer,
- Controls between the layers of end-tier systems,
- Scanning of organization's networks, systems and applications in regular time intervals,
- Monitoring networks, systems and applications for unauthorized access or anomalous behavior,
- Log records of security-related activities such as hardware and software configuration, changes and access attempts,
- Enforcement processes for password change management.

Beyond these requirements, confidential, personal or sensitive data are not encrypted and associated encryption keys are not properly protected by the organization. There is not an authentication system in place that applies higher levels of authentication to protect resources with higher levels of sensitivity.

6.5 General Overview

Apart from the specific results about essential components of information security, a general overview for whole organization was also provided by the assessment tool in order to present whole capabilities and requirements. In this context, general overview for the information security approaches of the defense industry organization is demonstrated in Figure 3.

As it can be seen in Figure 3, risk management approaches and processes are prominent components (respectively with the rates of 100% and 93%) for the organization. Technology is the third component with the rate of 88% while people is fourth (77%). On the other hand organizational reliance on IT is quite low because of the defense industry's nature and some security measures applied by the organization.

In the light of the assessments, scoring section of the assessment tool indicates that organizational reliance on IT of the defense industry organization is in medium level and overall assessment shows that organization is in good level with 300 points calculated based on the responses for each section of the assessment tool.

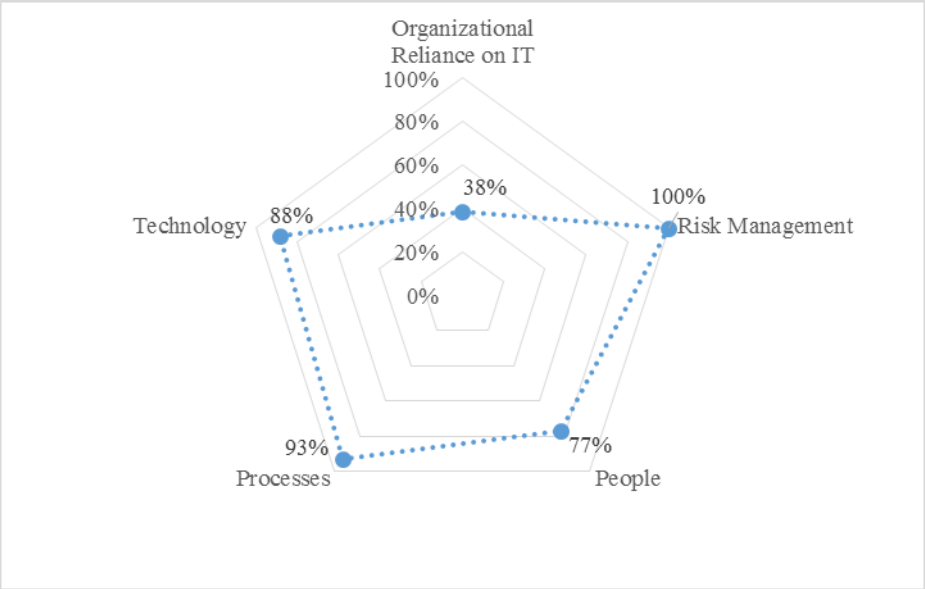

Fig. 3. General overview

7 Conclusion and Recommendations

Information security is an important factor for all types of organizations. Moreover, defense industry is one of the most important sectors for risk and information security management in changing technological conditions. Implementation and adaptation of the information security standards and policies are essential factors for organizations in the defense industry. Additionally, it can be said that measurements and analysis that reflect current situations are important and utility factors as well. In this context, the results generated from the tool provided a detailed insight for information security approaches of defense industry organization in terms of IT reliance, people, processes, risk management and technology.

The results of our study with respect to information security applications show that major applications were implemented by the defense industry organization. Furthermore, organizational reliance on IT for the defense industry organization is in low level by the reason of the security measures. Additionally results reflect that the defense industry organization is among the medium scaled companies and its approaches are in good level. On the other hand the organization has a stronger profile in terms of risk management and technology factors of information security.

In light of the results of this study, it can be suggested that attempts and some improvements should be made to increase effectiveness of information security approaches. These attempts can be listed as follows:

- Personnel requirements should be met for liaising with business units to identify any new security requirements based on changes to the operations.

- Policies that comply with information security policy, standards and regulations should be developed for all managers and senior managers.
- Interoperability of information security functions with other critical assets and functions should be provided to improve information security and privacy policies and applications.
- Education and training programs should be implemented for all employees.

Results about processes show that, information security, privacy programs and performance metrics should be completely evaluated and tested for each business units. Additionally, policy development and update analysis should be entirety implemented.

Technological approaches are another stronger side of the defense industry organization. Assessments reflect that authentication system that can be applied to higher levels of authentication to protect resources should be implemented. Data encryptions and associated encryption keys should be protected via new information security approaches as well.

References

1. Blackley, B., McDermott, E., Geer, D.: Information Security is Information Risk Management. In Proceedings of the 2001 Workshop on New Security Paradigms. pp.97--104. ACM, New York (2001)
2. Canbek, G., Sağıroğlu, Ş.: Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir Inceleme [An Evaluation on Information, Information Security and Processes]. Politeknik Dergisi, 9(3), 165--174 (2006)
3. Doğantimur, F.: (2009). ISO 27001 Çerçevesinde Kurumsal Bilgi Güvenliği [Organizational Information Security within the Framework of ISO 27001]. Unpublished thesis of professional competence, Ministry of Finance (2009)
4. Vural, Y., Sağıroğlu, Ş.: Kurumsal Bilgi Güvenliği ve Standartları Üzerine bir İnceleme [A Review on Organizational Information Security and Standards]. Gazi Üniversitesi Mühendislik ve Mimarlık Fakültesi Dergisi, 23(2), 507--522 (2008)
5. DPT: e-Dönüşüm Türkiye Projesi Birlikte Çalışabilirlik Esasları Rehberi [e-Transformation Turkey Project Principles of Interoperability Guide]. Devlet Planlama Teşkilatı, Ankara (2005)
6. DPT: Bilgi Toplumu Stratejisi Eylem Planı (2006- 2010). [Information Society Strategy Action Plan (2006- 2010)]. Devlet Planlama Teşkilatı, Ankara (2006)
7. Bilisim, http://bilisim2023.org/index.php?option=com_content&view=article&id=189:tuerkyede-blg-guevenl-yatirimlari-artiyor&catid=7:goerueler&Itemid=18
8. Thomas, G.: A Typology for the Case Study in Social Science Following a Review of Definition, Discourse and Structure. Qualitative Inquiry, 17(6), 511--521 (2011)
9. Zainal, Z.: Case Study as a Research Method. Jurnal Kemanusiaan Bil 9, 1--5 (2007)
10. Scarfone, K., Souppaya, M., Cody, A., Orebaugh, A.: Technical Guide to Information Security Testing and Assessment: Recommendations of the National Institute of Standards and Technology. Gaithersburg: U.S. Department of Commerce, Gaithersburg (2008)
11. Risk Assessment Toolkit, http://www.cio.ca.gov/OIS/governmen t/risk/toolkit.asp

Risk Assessment Toolkit, http://www.cio.ca.gov/OIS/governmen t/risk/toolkit.asp
Scarfone, K., Souppaya, M., Cody, A., Orebaugh, A:. Technical Guide to Information Security Testing and Assessment: Recommendations of the National Institute of Standards and Technology. Gaithersburg: U.S. Department of Commerce, Gaithersburg (2008).
Smith, T.F., Waterman, M.S.: Identification of Common Molecular Subsequences. J. Mol. Biol. 147, 195--197 (1981)
2. May, P., Ehrlich, H.C., Steinke, T.: ZIB Structure Prediction Pipeline: Composing a Complex Biological Workflow through Web Services. In: Nagel, W.E., Walter, W.V., Lehner, W. (eds.) Euro-Par 2006. LNCS, vol. 4128, pp. 1148--1158. Springer, Heidelberg (2006)
3. Thomas, G. (2011). A Typology for the Case Study in Social Science Following a Review of Definition, Discourse and Structure. Qualitative Inquiry, 17(6), 511--521 (2011)
Foster, I., Kesselman, C.: The Grid: Blueprint for a New Computing Infrastructure. Morgan Kaufmann, San Francisco (1999)
4. Vural, Y., Sağıroğlu, Ş.: Kurumsal Bilgi Güvenliği ve Standartları Üzerine bir İnceleme [A Review on Organizational Information Security and Standards]. Gazi Üniversitesi Mühendislik ve Mimarlık Fakültesi Dergisi, 23(2), 507--522 (2008)

Czajkowski, K., Fitzgerald, S., Foster, I., Kesselman, C.: Grid Information Services for Distributed Resource Sharing. In: 10th IEEE International Symposium on High Performance Distributed Computing, pp. 181--184. IEEE Press, New York (2001)

Foster, I., Kesselman, C., Nick, J., Tuecke, S.: The Physiology of the Grid: an Open Grid Services Architecture for Distributed Systems Integration. Technical report, Global Grid Forum (2002)
6. Zainal, Z.: Case Study as a Research Method. Jurnal Kemanusiaan Bil 9, 1--5 (2007)
)Bilisim,
http://bilisim2023.org/index.php?option=com_content&view=article&id=189:tuerkyede-blg-guevenl-yatirimlari-artiyor&catid=7:goerueler&Itemid=18
Risk Assessment Toolkit, http://www.cio.ca.gov/OIS/governmen t/risk/toolkit.asp