INFORMATION SECURITY STRATEGIES IN TURKEY: CURRENT STATUS, GOVERNMENT POLICIES & RECOMMENDATIONS

[1]GIZEM OGUTCU, [2]ESMA ERGUNER OZKOC

[1,2]Dept. of Management Information Systems, [1,2]Başkent University, Ankara, Turkey
Email: [1]ogutcu@baskent.edu.tr, [2]eeozkoc@baskent.edu.tr

Abstract: New communication technologies, social networks and electronic applications have made the life of the individual digital. So basically, the data is transformed into an e-entity that needs to be protected. Along with the digital movements of individual life, personal data began to circulate freely in these environments as uncontrolled masses. With all this, unreliable information security risks, cybercrime have begun to emerge, and individuals have had to protect themselves against digital life because of improper use of technology and low levels of awareness of individuals' information security threats.At the same time, the nations have to protect their citizens against all these threats and the possible consequences of these threats with the laws. In this regard, international cooperation has been made. When all this is taken into account, it is obvious how important information security is. This study describes the current situation, laws and strategies in Turkey regarding information security. In the study, strategies and information security that need to be developed have been explained with a visionary point of view regarding the individual, private sector and public context.

Keywords: Information Security, Turkey, Government IS Policies.

INTRODUCTION

Rapid development and cost reduction in information and communication technologies in recentyears has made these technologies much more accessible and usable. Accordingtothe 2017 surveydata, 3.731 billion (49.6%) of theworld'spopulation, which is 7.519 billionpeople, is usingtheinternet [1].Theincrease in Internet usagebetween 2000 and 2017 was 933.8%. InTurkey as a whole, the rate of having Internet accesswas76.3% in April 2016.Theproportion of regular Internet userswhomakeuse of the Internet at leastonce a dayor at leastonce a week is 94.9% in the first three months of 2016 [2].

The information-knowledge materialized through information technologies has made the globalization from an abstract phenomenon to a level that can be felt in the daily life of each individual.

Thus, the products of the visual, auditory, information-entertainment (infotainment) industry "idealized" by the digital networks "liberated" by the freedom of choice without intervention gained the necessary legitimacy in the legal dimension, not only technologically. It should be remembered that social life has a public dimension beyond the economic dimension that citizens and the state are confronted with.Therefore, as we have witnessed from the increasingly widespread e-government applications, digital networks become an important channel for public relations as well as for production and distribution relations [3]. All of these developments in this period of transition to e-government poses a danger in terms of national information security. In a study conducted in 2016, it was seen that the awareness of information security in Turkey, both individually and nationally, did not reach sufficient levels [4].In this context, many hardware and software protection methods have been developed based on information technologies to provide information security.This makes it difficult to obtain information from software or hardware exploits. Technical solutions have been developed and some threats have been removed. However, the recent exploitation of these deficits has left the place to the abuse of knowledge through the exploitation of the individual.

Social engineering, which is often heard and exemplified recently by threats, targets individuals who are the weakest link in security.Achieving information security is very difficult, and in this sense the weakest link in information security is people who are uneducated or lack of consciousness that are directly or indirectly exposed to the threat.Basically, security is not a product, it is a process [5]. Moreover, security is not a technology issue; it is a human and management problem.

As a matter of fact, the National Information Security Agency draft law proposal, which was introduced again ten years later, shows that these features of communication technologies are now more important both in terms of their impacts and the affected parties [3].Taken together, it is clear that the national information security strategy has a great influence on individuals, entrepreneurs and the public. In this study, developed strategies and policies on information security in Turkey were mentioned and a number of visionary proposals were given.

CURRENT STATUS & GOVERNMENTPOLICIES

This section includes the existing laws and regulations in Turkey. The relevant laws and their scope are explained.

2.1 Turkish Criminal Code (Law No. 5237)

In the Turkish Criminal Code numbered 5237, in addition to classical computer crimes related to information security such as entering a data

processing system, hindering, destroying or changing operation of a data processing system (Art. 243-244); abuse of bank or credit cards (Art. 245), qualified theft (Art. 142/2-e) and fraud (Art. 158/1-f), recording of personal data (Art. 135) and unlawful delivery or acquisition of data (Art. 136), destruction of data (Art. 138), prevention of communication (Art. 124), defamation (Art. 125), violation of communicational secrecy (Art. 132), tapping and recording of conversations between individuals (Art. 133), violation of privacy (Art. 134), indecency (Art. 226) are also described as criminal offences when information systems used [6].

2.2 Electronic Communication Law (No. 5809)

In Article 4/I of the code, it is regulated that electronic communication service and the secondary regulations to be made in this area are subject to the safeguarding of information security and communication secrecy. On the other hand, in Article 12 of the code gives operators the duty of ensuring confidentiality of 100/100 in the communication, providing uninterrupted service and maintaining the integrity of the network which are the key elements of information security [6]

2.3 Law of Intellectual and Artistic Works (No. 5846)

This provision specifically seeks to overcome the use of copyrighted works or licensed digital products by breaking certain protective programs used in the process of transporting, storing or publishing [6].

2.4 Electronic Signature Law (No. 5070)

A number of cyber crimes involving information security are covered under this Act. These offences are the unauthorised use of the electronic signature creation data mentioned in Article 16 of the law and fraudulent crimes in the electronic certificates framed in Article 17 [6].

2.5 Law on Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of Such Publications (No. 5651)

This law imposes a number of responsibilities and duties to provide of content, location, and access in the fight against crimes committed through the internet. Access blocking measures foreseen in the Act particularly provide for a partial fight against websites that distribute malicious software.

2.6Cyber Security Action Plan

The National Cyber Security Strategy and the 2013-2014 Action Plan, which are decided by the Cyber Security Council, are planned to prevent possible cyber attacks on organisations and institutions with critical importance by taking strategic decisions and action points.

When the Strategic Cyber Security Action Points examined, it can be seen that these points are collected under seven main headings which are;

1. Construction of Legal Regulations
2. Execution of the Assistance Activities for Judicial Processes
3. Establishment of an Intervention Organisation for National Cyber Events
4. Strengthening the Infrastructure of the National Cyber Security
5. Training Human Resources in the field of Cyber Security
6. Development of Domestic Technologies in Cyber Safety
7. Extension of National Security Mechanisms.

Under these headings, there are 29 action points and 95 sub action points that belongs them. There are a total of 31 institutions and organisations related to all these actions and responsible for these actions.

The decisions taken in the action plan aim to prevent possible attacks against the cyber environment and information systems throughout the country. Each passing day, along with the changes in attack methods depending on innovations in informatics, different vulnerabilities take place. In this action plan, targets haven been set in the direction of minimazing these vulnerabilities and becoming nationally secured information society. Because cyber attacks can be done easily and cheaply and it is difficult to determine the identification of the actor, user's awareness and training have been particularly emphasised, especially in action points. Also, user's freedom of expression is supported and they are encouraged to be ethical in cyberspace.

The 4th Article of the action covers the establishment of the National Cyber Emergency Response Team (TR-CERT) and Sectoral and Institutional Cyber Emergency Response Teams.

As a foundation to this article, in 11 November 2003, Communique on the Procedures and Principles for the Establishment, Duties and Activities of the Intervention in Cyber Events Teams is published to official gazette numbered 28818 by the Ministry of Transportation, Maritime Affairs and Communication.

2.7Prime Ministry Circular No. 2003/10 on Security Culture for Informations Systems and Networks

This guideline refers to the "Guiding Principles on the Formation of Security Culture" which is jointly adopted in 25 July 2002 by the member countries ofOrganisation for Economic Co-operation and Development(OECD) and it has been instructed to comply with OECD principles in order to raise the awareness of public on information security and take measures against the potential risks of information security [6].

2.8 Guidelines for the Interoperability Principles

"Guidelines for the Interoperability Principles" has been prepared under the coordination of the Undersecretariat of State Planning Organisation and with the contributions of public enterprises, private sector and non-governmental organisations in order to enable e-government services to be effectively presented to the citizens and the business world. One of the main policy of the guide has been identified as security. It has been determined that policies and regulations related to safety should be developed in the Guideline, which emphasises that the success of the services offered in the electronic environment are dependent on the achievement of an environment of trust.

In this respect in the security axis, some priorities such as:

• Establishment of information security management systems in all public institutions,

• If public institutions and organisations have confidential information in their information systems, the safety level of the devices they use in data transmission must conform to the common criteria standard,

• Dissemination of the electronic signature in e-government transactions,

• Extending cryptographic operations in classified correspondence,

• Determining the standards to be used for these measures have been included [6].

CONCLUSION & RECOMMENDATIONS

The importance of technology in terms of economic and social life has been understood by many countries today and knowledge-based economy transformation is one of the main targets in national strategies.On the other hand, it has become a clear requirement to prevent risks and threats to information and communication technologies and directly from technologies in order for this transformation process to continue smoothly.

In the context of national information security, countries and institutions produce strategies to protect their economic and socially beneficial information systems and critical infrastructures. The implementation of national strategies is based on an institutional structure in which both public and private sectors will work in coordination.New developments and trends in the field of public administration have required public administrations to design their future based on an institutional strategic plan.In this sense, the private sector has to act with a much more visionary view of the public in order to protect its own resources.

Legal Arrangement Studies in the Field of National Information Security, which has been in operation for almost 20 years in Turkey, have not been able to reach a desired result and have not been notified about the subject because of the fact that the concept of information security can not be understood completely and it is put into a wrong conceptual frame.

For this reason, when preparing strategies, it is necessary to develop a model that will cover not only the public or private sectors, but also all the individuals in society. The weakest link in information security in particular is always a people and systems can not be constructed independently of individuals.

While preparing the Sectoral and Institutional CEIT guides in Turkey, it is seen that the existing "Ciber Events Intervention Teams (CEIT)' Notification on Procedures and Principles for Establishment Tasks and Activities" is not sufficient.

For example, it is not clear how information communication between NCEI (National Ciber Events Intervention) and CEITs or between Sectoral CEIT and Institutional CEIT should be or how much information should be shared.Due to these and similar deficiencies, the related communiqué should be developed and published, and at the same time the mentioned guidelines should be updated.

These acts, which contain consequences such as unauthorized access to information systems, interruption of service delivery of the system, or corruption of the integrity of the system, are committed in the form of criminal offenses committed by criminal laws.Information crimes that have changed with the Internet are now being processed in the form of cyber crime, a more specific crime classification. Cybercrime is a crime that transcends national boundaries according to qualifications.It is possible that the people or groups that make up the cyber threat that goes to the information system and the tools used in a cyber attack (such as cybercriminal hosting, domain name, or server) are within the limits of more than one country.From this point of view, international cooperation is very important. The scope of contracts such as the European Cyber Crime Convention, which Turkey has also signed, needs to be expanded and revised frequently. Similarly, when it comes to technology, the speed of Turkish law is thought to be inadequate.For this reason, it is obvious that the context of information and technology should be evaluated differently in Turkish law and a different structure should be taken in this respect.Another important issue is that there are no national standards or indices that measure Information Security in Turkey.In cyber studies, the cultural impact is so important that it can not be denied.Turkish Culture is in a very favorable position for social engineering attacks because of many factors such as helpfulness in the context of information security.

All organizations, regardless of size and sector, are aware of the serious risks associated with cyber security.Despite this awareness, larger scale companies are exposed to more attacks each year.While risk is reaching global dimensions,

research shows that monetary losses have changed dramatically according to the scale of the organization [7].

Effective security awareness requires a commitment from the bottom to the top, communication and a strategy that most organizations do not have.Many institutions do not have an information security strategy. It is important to remember that focusing on rapid detection of security attacks and finding effective, timely intervention is very important for companies.When looking at today's connected business ecosystem, this step is as important as creating policies and processes for third parties interacting with the business.

A more aggressive policy in the area of Research and Development(R&D) and innovation is to be defined and a vision aimed at bringing Turkey into Europe's R&D center.In the R&D and innovation support provided for the software, the OECD guidelines: Frascati [8], Oslo[9] and Canberra[10] guidelines should be taken into consideration and the level of industry awareness should be increased in the context of these guidelines.

It is thought that it will be beneficial to make the following analyzes for all the mentioned developments. Accordingly, while a strategy is being developed in the context of information security;

Road Map:

i. Modelling
   - Current Situation Analysis, Technological Framework and Infrastructure, Internal Stakeholders, External Stakeholders, Technological Framework and Infrastructure, Information Security and System Security,

ii. Future Outlook and Targets,

iii. Temporary Plan in Short, Medium and Long Term,

iv. Mission, Vision and Working Principles,

v. Human Resources and Organization Strategy
   - Unit Organizational Model, Training and Support Strategy, Dissemination Strategy,

vi. SWOT Analysis,
   - Strengths, Development Areas (weaknesses), Opportunities, Threats

vii. PEST ANALYSIS
   - Political, Economic, Social Cultural Ecological, Technological

viii. Strategic Openings,

ix. Knowledge Management and Security Strategy,

x. Performance Criteria Method and Indicators,

xi. Costing

xii. Monitoring and Evaluation

xiii. Quality Management Strategy,
   - User Satisfaction and Recycling Assessment

It is considered beneficial to use the above road map while developing national information security strategies.

In summary, as mentioned above, the importance of information security strategy can not be denied. It is imperative for the public and private sector to cooperate and to be fed from foreign sources.In particular, the most important work to be done in this regard is the support of National Information Security technologies' R&Ds.The national production of critical technologies has great proposition in this regard.Apart from this, it is indisputable that unconditional awareness trainings must be given at every level of society at the individual dimension. It is also important that the elements of information security are a legal basis.In an environment where even the information of a patent-protected technology can be stolen through information crime, the criminal sanctions for the issue must be structured quickly. It is thought that all institutions should transfer information security to the corporate culture with an innovative business model.

REFERENCES

[1] (01.04.2017) Internet Usage Statistics, The Internet Big Picture World Internet Users and 2017 Population StatsRetrieved fromhttp://www.internetworldstats.com/stats.htm

[2] Türkiyeİstatistik Kurumu (01.04.2017) HanehalkıBilişimTeknolojileriKullanımAraştırması, 2016Retrieved fromhttp ://www.tuik.gov.tr/PreHaber Bultenleri.do?id=21779

[3] TörenliN.,(01.04.2017) KüreselleşenDünyadaBilgiGüvenliğiveTürkiyeRetrieved fromhttp://www.emo.org.tr/ekler/ae659bde981b0ad_ek.pdf

[4] Gizem Öğütçü, ÖzlemMüge Testik, Oumout Chouseinoglou, Analysis of personal information security behavior and awareness, Computers & Security, Volume 56, February 2016, Pages 83-93, ISSN 0167-4048, http://dx.doi.org/10.1016/j.cose.2015.10.002. (SCI)

[5] Sağsan, M. Bilgiteknolojilerigüvenliği: UlusalbilgininkorunmasınapragmatikbiryaklaşımveTürkiyeperspektifi. StratejikAnaliz, vol.2,no.22,s74-81 2002.

[6] [6]Güngör, M., (01.04.2017) Ulusal Bilgi Güvenliği: Stratejive Kurumsal Yapilanma Retrieved fromhttp://www.kalkinma.gov.tr/Lists/Uzmanlk%20Tezleri/Attachments/390/Ulusal%20Bilgi%20G%C3%BCvenli%C4%9Fi%20Strateji%20ve%20Kurumsal%20Yap%C4%B1lanma.pdf

[7] (01.04.2017)BilgiGüvenliğiveSiberGüvenlikHizmetleriYayınlarıRetrieved fromhttp ://www.pwc.com.tr/tr/hizmetlerimiz/risk-surec-teknoloji-hizmetleri/bilgi-guvenligi-ve-siber-guvenlik-yayinlari.html,

[8] Organisation for Economic Co-operation and Development (01.04.2017)Frascati Manual: Proposed Standard Practice for Surveys on Research and Experimental DevelopmentRetrieved fromhttp://www.oecd.org/sti/inno/frascatimanualproposedstandardpracticeforsurveysonresearchandexperimentaldevelopment6thedition.htm

[9] Organisation for Economic Co-operation and Development (01.04.2017) Proposed Guidelines for Collectingand Interpreting Technological Innovation Data Oslo ManualRetrieved fromhttps://www.oecd.org/sti/inno/2367580.pdf 01.04.2017

[10] Organisation for Economic Co-operation and Development (01.04.2017)Manual On The Measurement Of Human Resources Devoted To S&T"Canberra Manual"Retrieved fromhttp://www.tubitak.gov.tr/tubitak_content_files/BTYPD/kilavuzlar/Canberra.pdf

★★★