ÇANKAYA ÜNİVERSİTESİ

1997

THE OBSERVATION OF INFORMATION SECURITY AWARENESS IN TURKEY

AHMET DURMUŞ

SEPTEMBER 2014

THE OBSERVATION OF INFORMATION SECURITY AWARENESS IN TURKEY

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED
SCIENCES OF
ÇANKAYA UNIVERSITY

BY
AHMET DURMUŞ

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE
DEGREE OF
MASTER OF SCIENCE
IN
THE DEPARTMENT OF
COMPUTER ENGINEERING

SEPTEMBER 2014

Title of the Thesis : **The Observation of Information Security Awareness in Turkey**

Submitted by **Ahmet DURMUŞ**

Approval of the Graduate School of Natural and Applied Sciences, Çankaya University.

Prof. Dr. Taner ALTUNOK
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Assist. Prof. Dr. Murat SARAN
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Assist. Prof. Dr. Nurdan SARAN
Supervisor

Examination Date: 18.09.2014

Examining Committee Members

Assist. Prof. Dr. Nurdan SARAN	(Çankaya Univ.)
Assist. Prof. Dr. Sadık EŞMELİOĞLU	(Çankaya Univ.)
Dr. Hamdi M. YILDIRIM	(Bilkent Univ.)

STATEMENT OF NON-PLAGIARISM PAGE

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name : Ahmet DURMUŞ
Signature :
Date : 18.09.2014

ABSTRACT

THE OBSERVATION OF INFORMATION SECURITY AWARENESS IN TURKEY

DURMUŞ, Ahmet
M.Sc., Department of Computer Engineering
Supervisor: Assist. Prof. Dr. A. Nurdan SARAN

September 2014, 96 pages

In this thesis, information security awareness of five different sample domains has been examined by web-based general survey composed of basic security topics. Moreover, information security awareness of IT security personnel working in seven different public institutions which have great and complex network systems has also been examined by more technical survey as well. The correct and incorrect way of behaviour of respondents have been put forwarded in line with the discussion of information security principals by analyzing the responses with using well-known statistic analysis tool. Hence, the current posture of information security awareness has been spotted. The weak and strong sides of internet users in security knowledge have been emphasized with the analysis of general survey data. In the analysis of technical survey, the shortages of security measures resulted in some vulnerabilities in the institution networks have been highlighted. At the end of general survey, participants have been directed to relative website and a suggestion document has been also presented in order to contribute positively to their information security awareness at the same time.

Keywords: Information Security Awareness, Survey, Public Institution.

ÖZ

TÜRKİYE’DE BİLGİ GÜVENLİĞİ FARKINDALIĞININ İNCELENMESİ

DURMUŞ, Ahmet
Yüksek Lisans, Bilgisayar Mühendisliği Anabilim Dalı
Tez Yöneticisi: Yrd.Doç.Dr. A. Nurdan SARAN

Eylül 2014, 96 sayfa

Bu tezde temel bilgi güvenliği konularından oluşan web tabanlı genel bir anketle beş farklı örnek küme için bilgi güvenliği farkındalığı incelenmiştir. Ayrıca daha teknik bir anketle de büyük ve kompleks ağ yapısına sahip yedi devlet kurumumuzda çalışan, güvenlikten sorumlu bilgi işlem personelinin bilgi güvenliği farkındalığı da incelenmiştir. İyi bilinen bir istatistik analiz aracıyla anket katılımcılarının sorulara verdiği cevaplar analiz edilerek bilgi güvenliği prensipleri bakımından tartışılmak suretiyle doğru ve yanlış davranış şekilleri ortaya konulmuştur. Böylece, bilgi güvenliği farkındalığının mevcut durumu tespit edilmiştir. Bu bakımdan, genel anket verilerinin analiziyle internet kullancılarının bilgi güvenliği kültüründeki zayıf ve güçlü yanlar vurgulanmış; teknik anketin analiziyle ise devlet kurumlarımızın ağ yapılarında eksik güvenlik önlemleri sonucu ortaya çıkan zafiyetlere vurgulanmıştır. Genel anket sonunda katılımcılar, ilgili websitesi sayfasına yönlendirilerek ve ayrıca öneriler dökümanı sunularak aynı zamanda farkındalıklarına pozitif katkı sağlanmıştır.

Anahtar Kelimeler: Bilgi Güvenliği Farkındalığı, Anket, Devlet Kurumu.

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to Assist. Prof. Dr. A. Nurdan SARAN for her supervision, special guidance, suggestions, and encouragement through the development of this thesis.

It is a pleasure to express my special thanks to my family for their valuable support.

TABLE OF CONTENTS

CHAPTERS:

LIST OF FIGURES

FIGURES

LIST OF TABLES

TABLES

LIST OF ABBREVIATIONS

AAA	Authentication Authorization Accounting
ACL	Access Control List
ADSL	Asynchronous Digital Subscriber Line
ARP	Address Resolution Protocol
BPDU	Bridge Protocol Data Units
CISO	Chief Information Security Officer
COBIT	Control Objectives for Information and Related Technology
CPP	Control Plane Policy
DHCP	Dynamic Host Configuration Protocol
DLP	Data Loss/Leak Prevention
DMVPN	Dynamic Multipoint Virtual Private Network
DoS	Denial Of Service
DSL	Digital Subscriber Line
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol Over Local Area Network
FTP	File Transfer Protocol
GARP	Gratuitous Adress Resolution Protocol
GLBA	Gramm-Leach-Bliley Act
HIDS	Host Intrusion Detection System
HIPAA	Health Insurance Portability and Accountability Act
HIPS	Host Intrusion Prevention System
HTML	Hypertext Markup Language
HTTP	Hypertext Terminal Protocol
HTTPS	Secure Hypertext Terminal Protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	International Electrical Electronics Engineers
IM	Internet Messaging
IPS	Intrusion Prevention System

MAC	Media Access Control
MACSec	Media Access Control Security
NAC	Network Admission Control
NATO	North Atlantic Treaty Organization
NIDS	Network Intrusion Detection System
OSI	Open System Interconnection
P2P	Peer-to-peer
PCI DSS	Payment Card Industry Data Security Standards
Pentest	Penetration Test
PKI	Public Key Infrastructure
PwC	Pricewaterhouse Coopers
PVLAN	Private Local Area Network
RADIUS	Remote Authentication Dial In User Service
RAM	Random Access Memory
SaaS	Software as a service
SCADA	Supervisory Control and Data Acquisition
SPAM	Stupid Pointless Annoying Messages
SOME	Cyber Incidents Response Team (Siber Olaylara Müdahele Ekibi)
SSID	Service Set Identifier
SSL	Secure Socket Layer
SQL	Query Language
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access-Control System Plus
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TS ISO/IEC	Turkish Standard International Organization for Standardization/ International Electronics Commission
TUBITAK	The Scientific and Technological Research Council of Turkey (Türkiye Bilimsel ve Teknolojik Araştırma Kurumu)
TUBITAK-BILGEM	The Scientific and Technological Research Council of Turkey-Informatics and Information Security Research Center (Türkiye Bilimsel ve Teknolojik Araştırma Kurumu- Bilişim ve Bilgi Güvenliği Araştırma Merkezi)
UDP	User Datagram Protocol
URPF	Unicast Reverse Path Forwarding
USB	Universal Serial Bus
VLAN	Virtual Local Area Network

VPN	Virtual Private Network
WAF	Web Application Firewall
WEP	Wired Equivalent Protocol
WIPS	Wireless Intrusion Prevention System
XML	Extensible Markup Language
XSS	Cross Site Scripting

CHAPTER 1

INTRODUCTION

During the introduction, the followings have been examined: the definition and importance of cyber security, security incidents in global that threaten national security, the benefits of internet, where to start in IS and the objectives which were achieved during this study.

1.1 Background

Cyber security is defined as all of the processes to protect information technology (IT) assets which make up cyber space, to ensure confidentiality, integrity and availability of systems in which information is processed, and to detect cyber security incidents and attacks to activate response mechanism against, and to recover these systems after possible cyber security incidents [1].

As the world becomes more network centric, security remains a major concern, however, cyber security, information security (IS) and data security have been taking place in most countries' agenda. Security concerns are not hitting the headlines due to engagement of state institutions and critical infrastructures (e.g. defense industry, health, energy, finance) in digital environment. Besides, cyber space has been also accepted as a potential 5th front line [2].

In time, many devices have been depending upon IP protocol, thereby the term "cyber security" should be evaluated with conscious of that those are potential target victims that might be exposed to cyber attacks. In addition, most of the states have been establishing cyber armies to protect its own privacy at defense side, and to execute intelligence studies and electronic warfare at offense side. On the other hand, extensively growing data repositories due to ever-increasing information flow and the idea of rapidly accessing these qualified data assets have been creating charm that any states can ignore. As a state, not allocating enough resources to protect these qualified data and disregarding the significance of the issue will absolutely bring about the weaknesses on the network systems and damage country image inevitably. To stress the importance of the issue once again, in 2011, US Department of Defense declared a statement that cyber security attacks can be considered as an act of war [3].

The security concerns become significant and understandable when we imagine a day that phone network and nuclear reactors could not operate, SCADA systems did not run due to cyber attack, and thereby electric supply system became disrupted, or banks, hospitals and air traffic control systems were not operable. Moreover, Wikileaks cryptos and documents that became public, disruption of government institutions and banking system in Esthonia due to alleged Russian cyber attack, and then establishment of Cyber Defense Base of NATO in Tallinn, nuclear studies of Iran which was delayed for few years due to stuxnet virus, and claims of America about spyware found in Chinese network devices all emphasize that cyber security should be under the headline of national security undoubtedly [3].

From the perspective of end users, they can use available online banking transactions rather than going to branch offices. Citizens can easily benefit from governmental services via e-government environment in just a matter of time without waiting on a queue. They can shop online with credit card rather than going to the store. On top of that, people can announce their thoughts to the world and reach millions with the help of social media. All of these are revolutionary innovations that human being has faced in last decade. However, all of these innovations include risks as well as they ease daily jobs. Increasing number of devices connected to the largest network, the internet, means the wide range of devices can be exposed to cyber threats and shows as well how far the magnitude of risk is at the same time.

Having robust security posture is a requirement for minimization of economic expenditure, preserving data stock and maximization of prestige of diverse organizations [4]. In this regard, the questions can rise about how well-covered and precise security can be provided in place. In contrast to having state-of-the-art security technologies, many studies and researchers indicate that the weakest link in the chain, human, is the first place to start over because IS is not a technical issue at all but investing solely in technological infrastructure, equipments and experienced staff do not work well alone and the issue should be tackled as a whole. Despite all the high-end appliances and proper configurations are set for production network of public institutions, computers might still be infected with types of malicious software due to the lack of knowledge resulted in misuse or behavioral failure by administrative staff. So to say, trusted personnel who do not develop certain awareness level could pose threats that bad guy with bad intentions could not pose from outside of the network. The idea behind having secured perimeter is to start from human awareness.

From this point of view the main objectives of this thesis are as follows:

- ✓ Sample domains were composed of folks because human factor is the first issue to consider according to security philosophy and also many researchers, studies. To do so, two types of questionnaires were formed to apply. General questionnaire, which was composed of security fundamental topics, was applied online to internet users in Turkey, and technical questionnaire, which was composed of more in-depth technical questions, was applied to technical staff who have been working in public institutions.
- ✓ With the application of technical questionnaire, security measures that have to be taken in almost each layer of Open Systems Interconnection (OSI) were asked to IT team who are responsible for securing the network in 7 different public institutions, employing 1000 employees at least. The wide range of on-the-field network and system security topics were covered in technical survey, starting from some security features to configure in routers, switches, firewalls, intrusion prevention/detection systems (IPS/IDS) devices to physical security issues in system rooms. It highly contributed to implementation level of network.
- ✓ By the 60 questions in general questionnaire, internet users took part in to figure out how they response at times when they met security incidents and threats, or security breaches they caused. In the survey, their awareness was measured by several topics in different chapters like security incidents and

reporting, e-mail security, safely use of internet and computer, threats and preventive measures, password management and security, IS terms and social engineering.

- ✓ A downloadable document named as “IS Suggestions”, which was at the end of the online general survey, helped participants aware of some of the security issues by contributing their knowledge at the same time (Appendix D). With this document, we contributed to awareness of participants in addition to determination of current posture of ISA in Turkey.
- ✓ Once the participants have finished the survey regardless of if they have downloaded “IS Suggestion” document, they were redirected to TUBITAK-the Scientific and Technological Research Council of Turkey website www.bilgimikoruyorum.org.tr as a secondary option to make them awared of such ISA raising website which include audio visual educational scenarios issuing basic IS topics in daily life.
- ✓ Putting analysis aside, getting positive feedback from survey participants who were not interested that much in the security issues showed that this study contributed to information security awareness (ISA) positively.

1.2 Literature Review

According to National Institute of Standards and Technology [NIST] (2003) study, human is the weakest link in all attempts to secure network systems. This topic have been issued by many security communities in many reports, periodicals and conference presentations. In this regard, the study of NIST touches on how and what way the ISA trainings help employees realize IT responsibilities, organizational policies which are so important in enterprise wide. It is also addressed how enterprises build a security program by following a lifecycle approach. The very first step of lifecyle starts with awareness, then builds to training and evolves to education. To determine the requirements of an organization, awareness is the very first step that needs to be reviewed in consideration of change in the technology. It is a well-done reference study for organizations that would like to form a security program [5].

Adıgüzel C. G. (2009) apply a questionnaire, which comprise 23 questions, to 400 out of 2698 customers in Vakıfbank Maltepe Branch Office in his study titled “The effect of security worryings on internet banking use and a study upon Vakıfbank customers”. In respect to survey results, the ratio of internet banking use differs in terms of age, educational background and income level. Another result is that fraud and forgery which is mostly faced security incidents on internet do not improperly influence on internet banking use of customers [6].

Kruger, Drevin ve Steyn (2010) make an ISA raising questionnaire with 17 questions and survey with 44 students from two different African universities in their exploratory study. The questionnaire is composed of two main chapters. The first chapter is about vocabulary test to measure security awareness related to basic security terms. The second chapter focuses on behaviours to figure out how many participants turn theory into practice when they faced a security incident. According to survey results, the first chapter comprising vocabulary test help specify which training topics might be included in information security awareness program (ISAP). One quarter of participants do not know the “security incident” term. In regard to this result, they also do not know where to report security incidents for authority.
Most surprising result is that half of the participants do not know what strong password means. In the future, this exploratory study is thought to be carried out concerning private sector and some other places as a further work [7].

Öğütçü G. (2010) conduct a survey in which 881 persons take part, are drawn from students, administrative staff and academic personnels at Başkent University. The crucial result is that most of respondents do not report security incidents to any authority because they do not know where and how to report security incidents or crimes they met. Another issue is that the ratio remains very low as far as if the respondents follow up-to-date legal developments are concerned. Lastly, the awareness level of respondents who have awareness training is higher than who do not take. Generally, the awareness level of respondents are not that much high [8].

A web security awareness questionnaire with 4 questions is led by TUBITAK BILGEM- Informatics and Information Security Research Center surveying with 29 participants who are drawn from public institutions within the context of national information security. The survey is conducted in correspondance with web security training provided by TUBITAK. In regard to survey results, two stunning points stand out that 70 % of participants do not find high school/ university education well enough to gain the knowledge for using types of software securely. The second result express that %76 of participants do not find legal and politic tackles well enough for combating with security crimes and incidents [9].

Takemura (2011) carries out a web-based survey study in order to analyze the relation between ISA and behaviours in Japanese enterprises. Takemura comes to a result that participants who have lower awareness level are more likely to have problematic pattern of behaviour. In this regard, it is concluded that improving ISA absolutely direct people to behave correctly from the security point of view [10].

Veseli I. (2011) conducts a survey to measure the effectiveness of ISAP on users before and after awareness training, in the master thesis titled “measuring the effectiveness of ISAP”. Training course topics are composed of password protection and management, sensitive information handling, social engineering, physical/office protection, incident response. To give results, survey takers who join training courses have higher awareness level than who do not attend. Thus, Veseli concluded that awareness programs are beneficial and effective [11].

A. Bostan and I. Akman (2011) stress that user awareness and the behaviours which are gained are the weakest point by emphasizing human factor in the “4th Network and Information Security Symposium”. They also mention that there are many studies emphasizing that the users do not always act in accordance with what they believe and know although they have high technical level of awareness. The study briefly state that the habits of safe use need to be internalized and then to turn into behaviour. In the study, 466 persons answer the IS survey composed of 12 questions. 4 questions pertain to demographic features like age, gender, education and work experience which have meaningful influence on different number of factors and perceptions regarding to IT field literature. Independent variables (demographic features) and dependent variables (questions) are matched in order to establish hypothesis. In regard to computer security topic in the survey, the sensibility of respondents who are older decrease while the sensibility and awareness increase in accordance with the increase in work experience and training. The most surprising points are that when people get older they give more importance to web security. While females take care of computer security much more than males, males give more importance to web security than females do. The survey indicates that rise in user experience and education level help mitigate user-based security breaches and improving awareness [12].

Al-Shehri (2012) survey with 245 respondents coming from 35 countries with different background to measure ISA. Al-Shehri carry out the survey composed of 44 questions for about 1 month. The questionnaire is divided into 4 chapters such as demographics, computer general practice, security practice, security awareness respectively. 80 % of participants are graduate and post-graduate students. In regard to results, participants who attend IS training have higher security awareness in knowledge than who do not. For the future work, it is pointed that the number of females which comprise 20 % of all participants in the survey are needed to increase to get better analysis results [13].

Ministry of National Education in Turkey (2012) makes a survey study applying to 7484 employees working in the central and provincial organizations as soon as “Directive of Information and Systems” take effect in the ministry. The questionnaire is composed of 9 questions with some security topics such as password security and reporting IS incidents. In regard to survey results, 84 % of participants answer that they may share their passwords with administration. This result comes out a requirement that employees should gain habit for changing passwords. 30 % of participants change passwords when they suspect that it is stolen by somebody, while 24 % of participants do not change password anytime. In respect to setting a strong password, 42 % of participants do not set strong passwords while 31 % specify easy passwords not to forget [14].

I. Mart (2012), in her study titled “ISA in Information Culture”, carries out a questionnaire composed of 60 questions, the researcher survey with 501 individuals from different regions of Turkey from 4 different working titles such as medical personnel, lawyer, engineer and teachers between 2010 and 2012. She divides the survey into 3 chapters such as defining demographic features, ISA and technology use. In the chapter of defining demographic features, age, gender, educational status and occupation are asked. Researcher examine whether each demographic feature has a meaningful difference with computer and internet use, information awareness and/or information culture. She comes up with a result that IT use do not change in accordance with gender, age, educational status and occupations but ISA do change in accordance with age and occupation. Therefore, 25-34 years old people lack in security knowledge, and they need awareness training. 45 years and above are much awared of security because most of them are engineers and need to use technology in the job. For the future work, she points out that the results of this study might be compared with another study that will be able to conduct with different sample and space [15].

Deloitte-NASCIO (2012) runs a cyber security survey with public sector business leaders from 48 states and 2 territories. The study openly calls for collaboration and compliance against emerging threats because the states are at risk. To the daunting results of study, only 24% of CISOs are confident in protecting state's information assets against external threats. 14% of CISOs feel that they receive adequate funding for security. Only 32% of CISOs think that their team have the required cybersecurity competency. On the other hand, people change but the problems are persisting in comparison with the results of survey in 2010. It is also emphasized in the study that there are top 5 challenges when fighting against cyber threats are: emerging technologies, lack of visibility and influence within the enterprises, inadequate availability of cybersecurity professionals, increasing sophistication of threats and lack of sufficient funding. Gathered from the same study that CISOs are providing more training to staff to close cybersecurity skills gap as compared to results of 2010 survey [16].

M. Kocamustafaoğulları (2013), in her study entitled "A prototype for assessment of information security awareness and implementation level", emphasize that human is the weakest link in the security chain, and information security awareness and necessity are not understood well in organizations. It also stress that this kind of knowledge is a must need to be embraced by board of directors in order to build robust IS management and culture within the organization. In this regard, she designs a Turkish web-based prototype tool run on a server, based upon international security standards ISO/IEC 27001 and 27002, which is also composed of questions issuing security fundamentals that help organizations specify their IS requirements, and measure and evaluate them. In the survey module of the evaluation tool, users are asked to answer 24 questions composed of 8 particular security chapters. By applying the survey, answers made by respondents are evaluated over out of 5 points according to predefined ISA threshold of the organization in order to calculate organization awareness and application level. Questions in the survey concern diverse topics such as IS institution approach, security of information resources, security of human resources, physical and peripheral security, communication and IS execution, IS access control, development and maintenance management, IS incident management, business continuity, IS compatibility and monitoring management. In addition, the evaluation tool is tested by experts working in finance, public, consultancy and education sector. She comes up with an idea that it would be effective for this study to be supported extensively by non-profit and public authorities concerning with IS issues for future works [17].

Pricewaterhouse Coopers (PwC) company (2013), in the survey named "Key Findings From The Global State Of Information Security", execute 40 questions survey to apply to 9600 respondents including business and IT executives which are drawn from 115 countries and 11 diverse sectors for about 2 months, concerning the topics like privacy, IS safeguards and its business compatibility. 39% of participants who work in 500 million dollar revenue enterprises at least. 36% of participants are from North America, 26% Europe, 21% Asia-Pacific, 16% South America, 2 % Middle East and Africa. One of the remarkable results in the survey is that executives elevate the importance of security. Detected security incidents increase 25% while average financial costs increase 18% over last year. It is also given place to the opinions of IT executives in the survey. "…It's important to note that insider threats are not necessarily a 'bad guy' with bad intentions; it could be a good employee doing righteous work in an insecure manner. Our problems are more human than technological", Michael A. Mason, Chief Security Officer for Verizon Communications says by stressing human factor. In respect to this, he confirmingly says that 31 % of current employees and 27 % former employees are responsible for insider attacks. Briefly, most of respondents claim the same opinions. Only 4 % of respondents say that attacks are sourced from outside foreign countries [18].

Ernst & Young Global Ltd (2013) run a survey in 64 countries from 25 diverse sectors in its study named “Under Cyber Attack EY’s Global Information Security Survey 2013”. Totally 1900 respondents take part in the survey for a month. The methodology used to accomplish the survey is the interview. When it is not possible, online survey is held. CEOs, CIOs, CISOs and CFOs as well participate from different companies. There are some remarkable results which are gathered at the end of survey analysis. The organizations do know the depth and extension of cyber threats in all of their departments. Three fourths of respondents indicate that security policies are embraced by management staff. 43 % of respondents state that investments on IS increase while some others state that budgets do not address the cyber risks well enough. Even though innovations arise among organizations, they attribute the reasons of why the systems are subjected to cyber risks to the weak technology configuration and processes (e.g. patch management, threat intelligence) that do not meet today’s needs. It indicates why security management processes of companies are not mature yet. 68 % of respondents also state that business continuity and disaster recovery will be the top priority security issues for next year. Cyber risk, threat, data leakage/loss prevention, IS transformation and compliance monitoring are supposed to be other next 5 top security issues. Only 23 % of respondents also rate ISA and training as first and second top priority. More surprisingly 32 % of respondents see it as a last priority issue though it is the key component of improving and development security activities [19]. In this regard, it may be an indicator of that ISA could not be stated and apprehended well.

CERT Australia (2014), carries out an online survey study with 26 questions. Respondents come from 135 businesses that partner with CERT. The survey builds on the findings of 2012 and provides more comprehensive understanding about cyber security posture and threats. Some of concerns, vulnerabilities and areas to improve are noted at the end of survey. Most noticeable ones are that 95% of respondents think general staff need to improve their IT security skills/practices. More than 60% of respondents think IT staff, the board of directors need to improve IT security skills. To one of the results in the study, human factor is again one of the weakest point to care that the main internal factors that helped arise cyber security incidents are staff errors/omissions (57%) and poor security culture (50%). 16% of organisations do not employ staff dedicated to IT security, and the most of large organizations (72%), which have 200 and more employees, only have small IT security areas [20].

1.3 Problem Description

As mentioned in Literature Review, most of studies emphasize that human is the weakest link in the chain of security [6-19]. An employee can lack in knowledge to behave in parallel with IS principals resulting in undermining the network security within the organization even if the network structure is equipped with most high-end technology. Because of that reason, all personnel should be trained at regular intervals to improve security awareness. The study "*Building an Information Technology Security Awareness and Training Program"* conducted by NIST states:

"Learning is a continuum; it starts with awareness, builds to training, and evolves into education" [NIST, 2003].

But even if security awareness training is held by many organizations, it does not make employee change in behavior. The main purpose of ISAP should not only be to teach desired stuff but also to expect them not to repeat same faults in security practice. By doing so, proper effective security awareness questionnaire or tests should be applied before and after the training to measure how far the employees passed training stuff on their behaviours. However, awareness questionnaire should be subjected to change according to enhancements in technology. Another thing to consider is to create seperate questionnaires based on employees working in different departments. You can not get expected desired results from employees coming from different backgrounds and departments when you apply questionnaire with same content in a same way. The best way to get desired results is to specify training requirements, the way of appropriate training expression and content for specific groups by classifying groups.

In this respect, two different questionnaires were applied to two different groups of people in this study. Technical questionnaire, as it name implies, targeted on employees from technical backgrounds working in IT departments of public institutions, and the general questionnaire was composed of security basic topics which were applied to five different domains that are mentioned in Sub-problem Statements. Both of two surveys were prepared to test the knowledge, attitude and behaviour of participants from diversed backgrounds to put forward the ISA level. General questionnaire was much more based on testing knowledge and behavior in several security topics while technical questionnaire intends to test if IT staff did take proper security measures in network devices of public institution network.

1.4 Problem Statement

General questionnaire was carried out in order to solve the main problem below:

1st problem: Which ISA level do internet and computer users in Turkey reside in?

And technical questionnaire was carried out in order to solve the problem below:

2nd problem: Which ISA level do employees, who are responsible for managing great and sophisticated network systems (which in our case it is about 1000 end-users and above) in 7 public institutions of Turkey, reside in?

1.5 Sub-problem Statements

In this section, the main problem for general questionnaire mentioned above was divided into 5 sub-problems according to four options in 7th question, “Which sector-department do you work in?” and plus an option – students/graduates who answered “No” in Q6, “Do you work?”

Those four options which come from Q7 are named respectively as “I work in IT sector-IT department”, “I work in IT sector and non-IT department”, “I work in non-IT sector and IT department”, “I work in non-IT sector and non-IT department”. And the option comes from Q6 named as “Students/graduates”, that is non-workers in other words.

The employees who have been working in these four types of different backgrounds and students who have not been working were separately evaluated for measuring the

ISA level. It makes 5 subproblems to evaluate in total. These participants are already computer and internet users at the same time.

5 sample domains will be coded alphabetically in consecutive order to provide precise and smooth understanding inside the evaluation of the hypothesis in later chapters.

Sample domain A (SD-A): Employees working in IT sector and IT department.
Sample domain B (SD-B): Employees working in IT sector and non-IT department.
Sample domain C (SD-C): Employees working in non-IT sector and IT department.
Sample domain D (SD-D): Employees working in non-IT sector and non-IT department.
Sample domain E (SD-E): Students or graduates who are not working.

SP 1: Which ISA levels do employees in SD-A reside in?
SP 2: Which ISA levels do employees in SD-B reside in?
SP 3: Which ISA levels do employees in SD-C reside in?
SP 4: Which ISA levels do employees in SD-D reside in?
SP 5: Which ISA levels do students/graduates SD-E reside in?

1.6 Purposes of the Research

There are two seperate surveys in this study:

General survey aims to measure ISA of individuals who work in IT sector or different sector from diverse departments. One of the objectives of this study-presenting downloadable document for survey respondents and redirecting them to TUBITAK website, which include set of IS awareness trainings, indicate why this study not only measure the awareness but it also provides awareness raising.

The purpose of technical survey intends to measure how far the security professionals working in public institutions, which employ 1000 clients at least, take security countermeasures and implement set of security configurations. In this respect, a kind of vulnerability assessment and analysis was made in 7 public corparations in Turkey. In this respect, 1000 hosts/end-users or employees mean that the network system that serves for them is sufficiently complex in design and great in size. Those institutions should have some of the common security technologies and configurations in use.

1.7 Limitations of the Research

Technical survey was conducted in March, 2013 concerning 7 public institutions which have large-sized network systems. Overally, 20 security professionals took part in the survey.

General survey study was conducted in April through June, 2013. The sample domain of general survey was composed of employees working in IT sector/non-IT sector and IT department/non-IT departments as well as students/graduates who do not work anywhere.

1.8 Assumptions

Questionnaires were supposed to be responsed intimately and objectively. The sample domain chosen among research space is assumed to be accepted as presentative. Researcher was supposed to proceed unbiased in the process of applying and analyzing the study.

CHAPTER 2

RESEARCH METHOD

2.1 Universe and Sample

As two different surveys were carried out in this study, the target groups differ from each other.

The sample domain of technical survey focuses on security professionals working in 7 public institutions which have large network system serving 1000 hosts at least. The names of the institutions involved in the technical survey are confidential because of security concerns. Additionally, the anonymity of the participants are also guaranteed. It would be contradictory to the main goal of this study which concern with such security topics if the names and participants are exposed.

The sample domain of general survey was composed of internet users working in IT/non-IT sector and IT/non-IT department and also non-workers who are just as regular students/graduates. It was divided into 5 different categories so as to evaluate ISA level of each. The 5 subdomains of sample domain are shown below:

- Employees in IT sector and IT department (SD-A).
- Employees in IT sector and non-IT department (SD-B).
- Employees in non-IT sector and IT department (SD-C).
- Employees in non-IT sector and non-IT department (SD-D).
- Students or graduates who are non-workers as well department (SD-E).

2.2 Motivation

From the perspective of society, disregarding the security topics and developing knowledge only by acquiring hearsay have been leading to user misuse. Putting society aside, lack of awareness among technical personnel working in public institutions may even be able to harm the national interests. Recently compromised network systems in public institutions were one of the starting points to prepare such study.

As far as these motivations were concerned, security professionals managing great and sophisticated network systems in public institutions became target of the study. In this regard, they were asked to response the checklist-like questionnaire, which can be inspired by these public institutions or be improved further. By regarding the reality of that human factor is the very first step to focus on; a general questionnaire was carried out as well as technical questionnaire in order to outline the current status of public in this thesis.

Let’s touch on some statistics that motivate further;

According to Global Bot Infection Rate survey (2010), it was reported that bot infection rates in Turkey were highly above the world average numbers. Average global bot infection rates were 4.0 and 3.2 respectively at first and second quarters of 2010. The situation in Turkey was worrisome that 5.8 and 4.7 were the rates of first and second quarter of the same year [21].

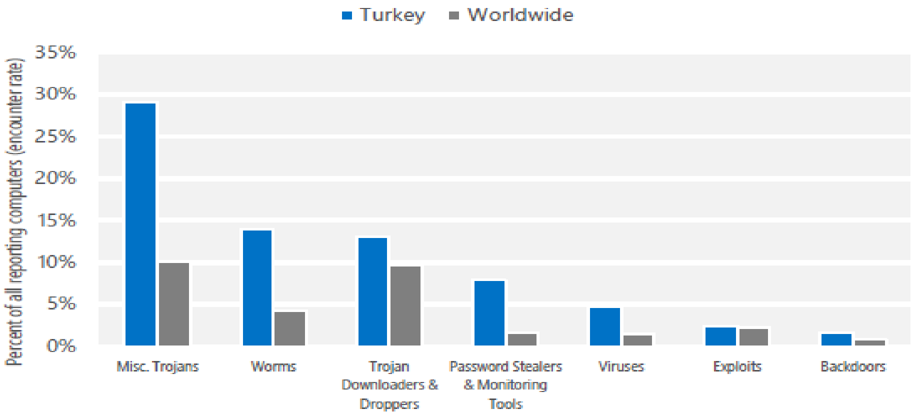


Figure 1 Threat categories (Microsoft research)

In Figure 1, most notable result was that Turkey is a convenient environment regarding to miscellaneous trojans. Average worldwide rate was about 10 % while the rate was 29.1 % in Turkey, which three times the global rate. Another important aspect was that the worms encounter rate in Turkey was roughly four times the global rate. Obviously, Turkey was considerably higher rates than worldwide rates in terms of the rest of the threat categories in Figure 1 [22].

In regard to the global threat report pursued by McAfee Labs, global top network threats and their sources in global were specified in the first quarter of 2012. As shown in Figure 2, SQL Injection and procedure call took the top two spots among network threats landscape.

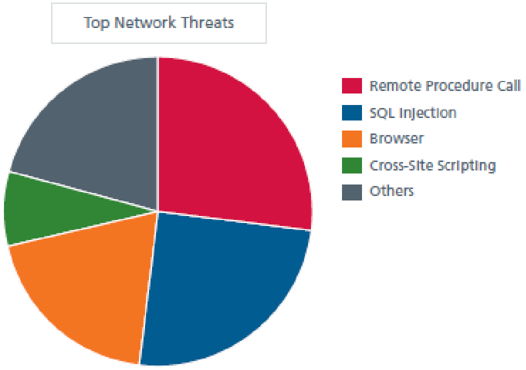


Figure 2 Network threats in 2012 (McAfee research)

In respect to SQL Injection threat, Turkey was at the first four while United States took the first place as the source of attacks as shown in Figure 3 below [23].

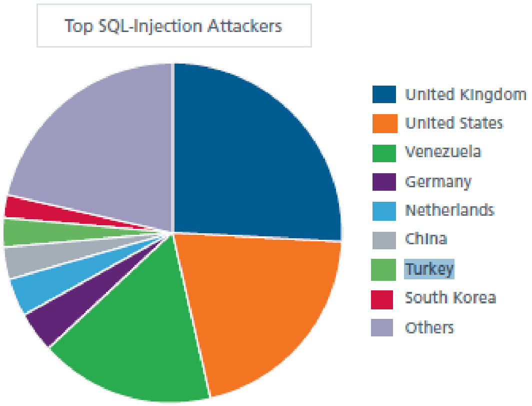


Figure 3 Top SQL-Injection Attackers

Analyzing the similar study named Global Malware Infection Rates, conducted by Microsoft in 2013, it was reported that malware encounter rate in Turkey is 44.9% while worldwide average rate was 21.6% (Figure 4). Encounter rate is defined as any malware attempts whether succeeds or not that was faced by Microsoft security products. Additionally, malware infection rate in Turkey was 25.2 % while global average rate was 17.8% in last quarter of 2013. Even more, in infection rate graph, it peaked at over 15% with the increase of more than 10 % along with last quarter of the year [21]. Considering the analysis, it was hard to claim that Turkey's security posture was cheering in terms of several threat categories in past years.

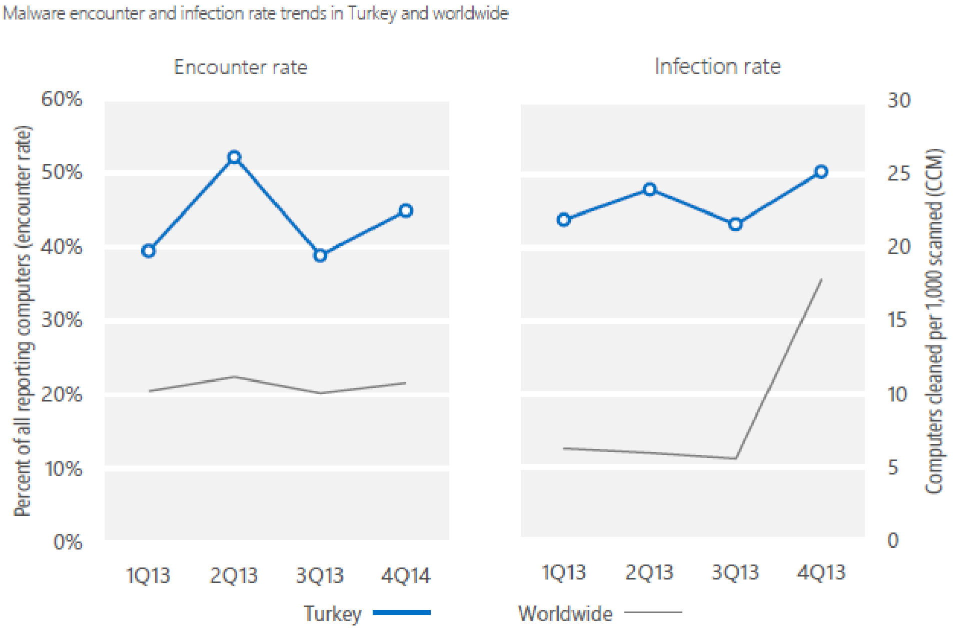


Figure 4 Malware encounter and infection rates in 2013

2.3 Forming Questionnaires

In this section, the paces when forming both 2 questionnaires and the types of questions in the surveys are discussed. The overall study especially in designing surveys was carried out under the supervision. The surveys were firstly tested as pilot work. Later on, they were presented to supervisor and some experts who have been working in security field to get proper feedback.

2.3.1 Technical questionnaire

Technical questionnaire focused on security professionals working in 7 public institutions which have great network systems in size serving 1000 hosts or above. Known that the network systems in public institutions, which have been exposing some vulnerabilities in security configurations and/or been lacking knowledge or awareness, have hit the headlines in recent years. Even if there was not, these kinds of awareness raising activities like in this study and even more have been arranged comprehensively at regular intervals by many awared countries as mentioned in earlier chapters.

First of all, before achieving the last technical survey type, more technical questionnaire was considered to be prepared to contribute to the implementation level of network by directing security personnels for questioning major security configuration sets and commands in network devices such as firewalls, routers, switches, IPS/IDS devices and so on. But when the great data centers of public institutions were imagined, there was going to be numerous different of vendor products which have different types of command sets. This type of survey which will be composed of questions examining diverse command sets of network devices of different vendors was not going to be applicable and also participants were going to have difficulty in responsing such survey or were going to reject kindly because the survey was going to be considered as security violation, a kind of reconnaissance of institutions' network as well. If this had been the case, the main purpose of the study would have appeared to be conradicted what the name of the study implies, that is, we would have violated IS while contributing to ISA with this study. Therefore, it was concluded that this kind of survey can not be done.

Secondly, a type of survey which addresses more verbal questions was thought to be formed. By doing so, literature study was made to add information/system/network security questions to the question bank. Relevant websites and security quizzes and tests were searched for populating the question bank. Then, the question bank was polled enough and reduced from irrelevant questions and options. The survey was presented to security experts working in the field as a pilot study in order to get their opinions. We agreed with security experts that the survey was including so many specific questions that can not be responsed easily. Therefore, this survey study as well was ignored because expecting healthy and satisfactory results was going to be so optimistic.

At last, the latest technical questionnaire was composed of 10 chapters which concerned with security countermeasures needed to be taken in OSI layers and end-points. These were about indispensable security features to be configured in all network devices and the measures to be taken in physical infrastructure in order to have adequate and optimal network security. The questions covered common security topics that should be present in every institution network. Question types and topics are briefly covered below. In some of the questions, there is a ‘skip logic’ functionality that does not show respondents the next question according to responses they made in previous question. The survey forms can be seen in Appendices in more detail.

First chapter comprises 5 questions that call for demographic features of respondents such as gender, age, educational background, work title and year of working experience.

Second chapter concentrates on security standards, procedures and training. It is composed of 9 questions. There is a skip logic in 10th question that enable participants skip the next question if they do not get ISA training in the institution because the next question is “how often do you arrange ISA training for your employees?”

Third chapter is the entrance to technical questions which are composed of 10 questions concerning with firewalls, IDS/IPS devices, management, penetration and traffic control. There isn’t any skip logic in here.

Fourth chapter is about wireless network security. It comprises 5 questions. There is a skip logic in 25th question that enable participants skip the next question if employees do not have any idea about the question or if they do not use wireless IPS appliances in the institution network.

Fifth chapter is about OSI Application Layer (Layer 7) security. It is composed of 2 questions related to voice applications. So there is a skip logic in the 30th question that enable participants skip the next question if they do not use voice applications in the institution network.

Sixth chapter pertains to OSI Transport Layer (Layer 4) security. This chapter is composed of only one question.

Seventh chapter concerns with OSI Network Layer (Layer 3) security. The chapter is composed of 2 questions.

Eighth chapter is about OSI Data Link Layer (Layer 2) security. The chapter is composed of 12 questions.

Ninth chapter is related to OSI Physical Layer (Layer 1) security. The chapter is composed of 14 questions.

Tenth chapter is the last chapter which is related to end-users' security, is composed of three questions.

The options of 42 questions in the survey were named as "Yes", "No", "Another technology", "I do not have any idea" respectively. The rest was formed as multiple choice questions with different options. There are 3 skip logics (or question piping) in the questions. In this respect, respondents were required to answer from number of 57 to 60 questions in total.

2.3.2 General questionnaire

General survey targeted 5 kinds of sample domains as explained earlier chapters. First of all, once again a literature review was made to determine whether such study had been done earlier. A question bank with 100 questions was formed by drawing from number of types of security tests, quizzes and master thesis [6-15] [24-25]. The questions in the bank were grouped by topics. Then, time-consuming questions and those requiring so much knowledge were eliminated. Additionally, the questions which were very similar to each other and decreased reliability of the survey were thrown out. Lastly, the current general survey was ready with 40 questions for pilot study. In pilot work, feedback questions were put at the end of survey form for robustness of the survey. They requested from respondents in pilot work if there was a question that they did not understand or that directed them to expected answers and that contained odd meaning. Finally, the pilot study was carried out with 35 computer engineer plus political science undergraduate students at Çankaya University and the professions from other fields.

General questionnaire comprise 7 chapters which have skip logics/question pipings in some questions as in technical questionnaire. There are 8 questions which have skip logics in total. Q4, Q6, Q9, Q13, Q15, Q19, Q28 and Q31 are skippable questions. To exemplify the skip logic, if a participant is an internet user who does not have an e-mail address, he/she does not have to answer the questions in e-mail security chapter. That's why skip logics were employed. The survey was considered as dynamic in this respect.

First chapter concerns with demographic features of participants such as gender, age, location, educational and working status, is composed of 8 questions.

Second chapter asks participants to response about security incident and reporting, social media and internet usage habits. This chapter comprises 10 questions. There is a skip logic and question piping in this chapter. For example; if a participant answered "No" in the 9th question, "Do you use internet?" in the survey, the survey was terminated without asking rest of the questions along the survey because the goal of the study is to measure ISA among internet users, thereby allowing the user who do not use Internet continue to survey would not make sense and would decrease the reliability of the survey. In a similar way, if a participant answered "Yes" in the 13th question, "Do you have any social media site account?", the participant was piped to the next question or skipped to 15th question otherwise. There was also some other questions to make possible to skip more than one question in accordance with the choice that the participant made. In this chapter, 5 point likert scale was also used in three questions. The points were "very few", "few", "average", "lot" and "very lot" in 10th question. In 11th question, the points scale were "certainly yes", "yes", “sometimes”, “no”, “certainly no” while “never heard”, “know little”, “averagely”, “know well” and “know very well” were the points for 12th question.

Third chapter is composed of 5 questions related to e-mail security. There is a skip logic here that there are 4 questions to answer if the participant uses an e-mail address. The question is skipped otherwise; however, survey respondents can skip 4 questions totally in this chapter.

Fourth chapter is related to “Using Computer and Internet Safely”, which comprises 4 questions. There is not any skip logic in this chapter.

Fifth chapter concerns with “Threats, Update and Backup, Antivirus and Firewall Use” which comprises 7 questions. There are skip logics in 2 questions in here. If the participants do not use file sharing software, relative next question is skipped. If the participants do not use antivirus software, next question related to antivirus software is skipped once again. The participants can skip 2 questions accordingly in total.

Sixth chapter is composed of 3 questions related to “Password Security”. There is no skip logic in this chapter.

Seventh chapter focuses on “IS terms and Social Engineering” comprising 3 questions which are more verbal-based than others. There isn’t any skip logic in this last chapter.

As far as skip logic/question piping functionality is concerned, a participant who answered “No” in 9th question, which asks if the user have used Internet or not, can only answer 9 questions because this survey is only for internet users as mentioned earlier. By hitting the skip logics in the options, a participants can only skip 6 questions at maximum, thereby they can answer 34 questions in total. If they did not hit any questions with skip logics at all, they can answer all 40 questions. Briefly, a survey participant could answer from 34- 40 questions. When 40 questions are taken into consideration at worst case, all of the questions can be answered in 15 minutes or below.

2.4 Data Gathering

There are two types of research methodology in literature: qualitative and quantitative approaches. Qualitative data gathering depends on interviews with participants like we did in technical questionnaire, that is, physical existence of the researcher is required to interact with respondents to complete the interviews. Quantitative data gathering depends on internet-based survey as conducted in general questionnaire.

2.4.1 Technical questionnaire

Numbers of 20 IT professionals, who have been working in 7 public institutions which have great and sophisticated network systems with 1000 hosts at least, were surveyed by making interviews with each of them. Before making interviews, permission was received by upper management of particular public institutions. Receiving permissions provided us to attract the employees' attention. There were different job titles in the public institutions that some of the employees were only responsible for securing the network while some of them were just network specialist and responsible for many tasks to perform in the IT department of the institution as well as securing the network. The interviews were made with only employees who were in charge of security issues in the network systems. All others already kindly refused to participate because they did not have security profession. Technical survey was prepared specifically to address the measures that employees are required to take to secure the network.

A resource was asked for guidance before the survey preparation [26-28]. Using proper and accurate meaning of the words, technical statements and expressions, avoiding from open-ended questions and directing respondents expected answers were some of the basic rules to care during preparation. Caring these rules made the survey clear to understand and made the participants response to questions on time as expected. If the rules mentioned in the resource were not followed, high drop-outs of the survey could happen. However, the completion time was around 10 minutes or below. The respondents were employed voluntarily.

Regarding the options in the questions, there are optional parts to fill in paranthesis in the options named “Other” or “We use another technology/method”. Number of 47 questions include these options. The participants who chose one of these options were free to fill those blanks, thereby they were not mandatory. All of the questions include multiple choices. When the technical survey study was finished, in analysis, there wasn’t any mismarked option in any question or a question that was skipped mistakenly. Lastly, the raw data was ready for SPSS input. The answers of 20 forms were typed into the SPSS one by one for analysis. All of the answers that IT personnel made and the names of the public institutions were treated as confidential information. Identifying demographic knowledge was never asked or collected from the respondents. Hence, the forms were randomly shuffled to ensure the anonymity.

2.4.2 General questionnaire

General survey was prepared on the website, “www.surveymonkey.com”. In the direction of predetermined time line, an interactive online web survey was conducted by accessing 545 internet users working in diverse jobs (IT sector/non-IT sector and IT department/non-IT department, and students/graduates) from different cities of Turkey. As only one of the participants said “No” in 9th question, “Do you use Internet?”. That response was removed and was not evaluated in the analysis. General survey only targeted internet users as mentioned earlier. In this respect, a survey taker could answer 35-40 questions in total. The participants were only allowed to answer per computer/IP address in order to prevent people from taking the survey more than once. On the other hand, even if a participant came to the last page of survey after answering all of the questions, the survey form was not accepted as completed yet unless the participant clicked the “finish the survey” button. Same survey rules were run in the general survey design as well as in technical survey. The completion time was not more than 15 minutes. The respondents were employed to the survey voluntarily. Facebook and twitter walls, e-mail invitations, e-mail groups and types of technology forums were used to deliver general survey to audiences. Finally, the raw data was ready for SPSS analysis. In here, there was no need to input every answer to SPSS tool because Surveymonkey has the functionality to export data as SPSS file format to analyze. Surveymonkey guaranteed the security of data in transit and storage as code of conduct.

CHAPTER 3

STATISTICAL ANALYSIS AND DISCUSSION

During this chapter, results of two surveys will be examined respectively. All of 40 questions in general survey will be usually analyzed by crosstabs and by frequency analysis if necessary while all 60 questions in technical survey will be analyzed only by frequency analysis test in SPSS tool. While making analysis, strong and weak side of the participants will be discussed and put forwarded what threats and vulnerabilities can arise accordingly. In this regard, this chapter will baseline the Conclusion and Future Works chapters.

3.1 Results of General Questionnaire

In this section, the frequency analysis of the questions of 7 chapters in the general questionnaire will be covered one by one. To recall, these chapters are named relatively as demographic features, security incidents and reporting, e-mail security, safely use of internet and computer, threats and preventive measures, password management and security, IS terms and social engineering.

While evaluating the each question, ISA level of employees working in different sector and departments will be revealed first. After that, ISA level of students/graduates who answered “No” in Q6, “Do you work?”, will be specified.

First of all, meaningful variables (questions), whose results calculated by Pearson Chi-Square test found to be significant; were determined by crossing with options in Q7 (five sample domains) in Table 2. The questions whose results are found to be insignificant, that is, which show similar distribution at rates among options will also be analyzed and discussed at the same time. Significancy means that only rate of specific option(s) obviously rised sharply in a question when we compared to other options in same question. Insignificancy means that the rates of options in a question are close to each other and show similar distribution when the rates of them are observed.

The evaluation criteria to determine which questions show significancy is the application of Pearson Chi-Square test. Confidence level was specified as 95 % that (1- α) = 0.95 which makes α = 0.05. Chi-Square value denotes as χ^2. The probability stands for *p*. If the *p* value for the calculated χ^2 is $p < \alpha$, null hypothesis is rejected. In other words, the relation between Q7 and Qx (any question) is found to be statistically significant, that is, the distribution of the rates gathered from the crosstab of Q7 and Qx is distinctive. If the p value for the calculated χ^2 is $p > \alpha = 0.05$, there is no significant results in terms of rates, thereby the rates of the options in crosstab between Q7 and Qx represent similar distribution. When regarding the ISA level, a type of scale was used. From the respondents who get certain rate were evaluated as following equivalent grades:

0-20 % is “Very unsatisfactory”, 20- 45 % is “Unsatisfactory”, 45- 70 % is “Average”, 70-85 % is “Satisfactory” and 85-100 % is “Very satisfactory”.

Only questions whose results are significant are shown in Table 2. Chi-Square values of the rest of the questions other than those in Table 2 are insignificant, that is, the rates of the options in those questions are close to each other. For clarity, the results of those questions found insignificant by Chi-Square will not be shown in a table.

To show how Chi-Square test is achieved, Q10 is illustrated below as an example:

In Q10, the significant value for Pearson Chi-Square was found 0.000. This is the lower than our threshold alpha value (0.05), however, the null hypothesis (H0) is rejected because the results of the question “how much time do you spend on the internet?” is found to be statistically meaningful onto sample domains in Q7 by Chi-Square test (Table 1). When the rates of the responses in Q10 are observed in the analysis of general questionnaire chapter, we can see that all of the sample domains showed much more tendency to mark only specific option(s) among other options (Table 8). The relative Chi-Square test is also illustrated in Table 1 below.

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	50.317[a]	12	.000
Likelihood Ratio	54.538	12	.000
Linear-by-Linear Association	33.566	1	.000
N of Valid Cases	408		

Table 1 A sample Chi-Square test for Q10

	Value	df	Asymp. Sig. (2-sided)
Q11	24.438[a]	12	.005
Q12	31.093[a]	12	.002
Q13	4.758[a]	3	.019
Q19	7.845[a]	3	.049
Q20	13.128[a]	5	.015
Q21	12.046[a]	9	.021
Q22	31.819[a]	9	.000
Q23	19.411[a]	9	.022
Q28	35.361[a]	3	.000
Q30	28.865[a]	9	,001
Q32	21.305[a]	12	.046
Q33	10.451[a]	12	.005
Q34	5.011[a]	9	.033
Q37	17.962[a]	9	.036

Table 2 The questions found significant by Chi-Square test

In the questions specified in Table 2 with Chi-Square test values, respondents have intensely concentrated on marking only specific option(s). The significance value- the rightmost is observed, all of them remain below the reference alpha value- 0.05 by confirming the results. Those questions whose Chi-Square value remained above the alpha value, the survey participants haven’t intensely concentrated on marking only specific option(s). Therefore, we will realize in next chapters that the difference between the rates of the options are not that high when compared to the questions in Table 2. Those questions will also be evaluated in next chapters.

3.1.1 Analysis of demographic variables

In this section, the main objective is to provide more general outlook to respondants' socio-demographic features, however, the questions starting from 1-8 will be discussed in terms of frequency analysis of demographic features such as gender, age, location, graduate degree, field of study in the school, employment status, sector and department and working experience which all comprise the first chapter in the general survey at the same time.

In some of the variables, one of the descriptive statistic techniques named "crosstabs" was used to describe the consistency of the ratio of the variables. Participants' age-gender, age-graduate degree and lastly working experience- sector and department were the independent variables which were crossed in order to evaluate the consistency between them. For the clarity, city and faculty records were not included.

Variables	Subvariables	Frequency	Percent
Q1. Your gender?	a. Male b. Female	425 119	78,1 21,9
Q2. Your age?	a. < 18 b. 18- 24 c. 25- 34 d. 35- 44 e. 45- 54 f. > 55	6 93 233 118 66 28	1,1 17,1 42,8 21,7 12,1 5,1
Q4. What is your (expected) graduate degree?	a. Primary School b. Secondary School c. High School d. Upper Secondary School e. Undergraduate f. Postgraduate g. Doctorate	1 5 54 31 350 85 18	,2 ,9 9,9 5,7 64,3 15,6 3,3
Q6. Do you work?	a. Yes b. No	436 97	81,8 18,2
Q7. Which sector-department do you work in?	a. IT sector- IT department b. IT sector- non-IT department c. Non-IT sector- IT department d. Non-IT sector- non-IT department	56 67 50 237	13,7 16,3 12,2 57,8

Q8. Your working experience?	a. 0-1 year b. 1-3 years c. 3-5 years d. 5-10 years e. Above 10 years	28 68 64 76 174	6,8 16,6 15,6 18,5 42,4

Table 3 Frequency analysis of demographic variables

When distribution of genders of the survey participants is viewed, most of the participants are composed of male. It is shown that male participants are represented 56.2% more than female participants. When it comes to ages of participants, the highest participant ratio is shown at 25-34 age group with 42.8 %. 35-44 age group comes second after that (Table 3). According to crosstab in Table 4, most of the participants are composed of 25-34 age group for both genders. More than half of the all participants reside in 25-44 age space. In addition to this, respondents who participated to survey are from various different cities. More than 75 % of participants are from Ankara. For the clarity, faculty and city information of the participants are not shown in the table.

Crosstab (Q2*Q1)		**Q1. Your gender?**		Total
		Male	Female	
Q2. Your age?	Below 18	6	0	6
	18-24	57	36	93
	25-34	185	48	233
	35-44	95	23	118
	45-54	58	8	66
	Above 54	24	4	28
Total		425	119	544

Table 4 Crosstabulation for age and gender

While the ratio of the participants who are undergraduate degree comprise the biggest participant category with 64.3 %, postgraduate degree and high school degree participants follow after with 15.6 % and 9.9 % respectively. This distribution indicates the correspondence with participants’ age distribution confirmingly that participants who are undergraduate degree are 25-34 year old when it is evaluated by crosstab (Table 5).

Crosstab (Q2*Q4)		Q4. Your graduate degree?							Total
		Primary Sc.	Secondary Sc.	High Sc.	Upper Secondary Sc.	Under graduate	Post graduate	Doctorate	
Q2. Your age?	<18	0	1	3	0	1	1	0	6
	18-24	0	1	5	5	74	7	1	93
	25-34	1	0	17	13	146	49	7	233
	35-44	0	0	13	6	75	17	7	118
	45-54	0	1	8	5	40	9	3	66
	>54	0	2	8	2	14	2	0	28
Total		1	5	54	31	350	85	18	544

Table 5 Crosstabulation for age and graduate degree

When the answers of participants for working status are observed, more than four fifth of the participants have a job. The participants who have a job in non-IT departments comprise more than 70 % of all. 57.8 % of employees work in non-IT sector and non-IT departments. The employees working in IT sector and IT departments are represented by 30 %.

Crosstab (Q8*Q7)		Q7. Which sector- department do you work in?			
		IT sector IT department	IT sector non-IT dpt	Non-IT sector IT dpt	Non- IT sector Non-IT dpt
Q8. Your working experience ?	0-1 year	7.1 %	10.4 %	7.8 %	5.5 %
	1-3 years	12.5 %	23.9 %	19.6 %	14.8 %
	3-5 years	14.3 %	20.9 %	31.4 %	11.4 %
	5-10 years	30.4 %	14.9 %	15.7 %	17.3 %
	>10 years	35.7 %	29.8 %	25.5 %	51.0 %

Table 6 Crosstabulation for Q8 and Q7

When working experience and sector-department is considered, the most over-experienced (10 years and above) employees reside in non-IT sector and non-IT departments. The finding may be resulted by the highest participant rate in non-IT sector and non-IT department. It may be concluded that more than 60 % of the employees working in IT sector and IT department have 5 years and above experience as well as employees in non-IT sector and non- IT department which gets the around rates (Table 6).

3.1.2 Analysis of security incidents and reporting

Variables	Subvariables	Frequency	Percent
Q9. Do you use internet?	a. Yes b. No	544 1	99,8 ,2

Table 7 Frequency Analysis of Q9

As discussed earlier, participants who do not use internet are not our target. Thus, it is provided among the survey that all of the participants are from internet users as shown in Q9. One person who answered “No” in this question was removed from the overall results for naturalization of raw data (Table 7).

Crosstab (Q7*Q10)			Q10. How much time do you spend on the Internet?					Total
			Very little	Little	Average	Much	Very much	
Q7. Which sector-department do you work in?	IT sector and IT department	% within which sector-department do you work in?	0.0%	0.0%	19.6%	41.1%	39.3%	100.0%
	IT sector and non-IT department	% within which sector-department do you work in?	1.5%	1.5%	23.9%	38.8%	34.3%	100.0%
	Non-IT sector and IT department	% within which sector-department do you work in?	4.2%	2.1%	12.5%	56.2%	25.0%	100.0%
	Non-IT sector and non-IT department	% within which sector-department do you work in?	2.5%	6.3%	43.9%	31.2%	16.0%	100.0%

Table 8 Crosstabulation for Q7 and Q10

Crosstab (Q6*Q10)		Q10. How much time do you spend on the Internet?					Total
		Very little	Little	Average	Much	Very much	
Q6. Do you work ?	Students / graduates (who answered as “No” in Q6)	2,1%	4.1%	42.3%	34.0%	17.5%	100.0%

Table 9 Crosstabulation for Q6 and Q10

In Q10, almost all of the employees spend much of their time on internet that it makes them potential targets in untrusted network- internet and makes IS concerns more important issues to know. All of the respondents working in IT sector and IT department answered this question as “average” and above scales that makes them first in comparison with rest of them (Table 8).

Most of the non-workers who are just students/graduates have been spending their time “averagely” and above (Table 9). Besides, more than 80 % of them do not trust in shopping at internet cafes, which is equivalent to “satisfactory” and “very satisfactory” ISA level (Table 11). Shown that all of the groups have mostly concentrated on specific options like “average” and “much”. The results of Q10 are confirmed by Chi-Square values in previous chapter.

Crosstab (Q7*Q11)			**Q11. Do you shop on the internet at internet cafes?**					Total
			Certainly yes	Yes	Sometimes	No	Certainly no	
Q7. Which sector-department do you work in?	IT sector and IT department	% within which sector-department do you work in?	7,1%	5,4%	5,4%	30,4%	51,8%	100.0%
	IT sector and non-IT department	% within which sector-department do you work in?	0,0%	6,0%	9,0%	34,3%	50,7%	100.0%
	Non-IT sector and IT department	% within which sector-department do you work in?	0,0%	2,1%	2,1%	35,4%	60,4%	100.0%
	Non-IT sector and non-IT department	% within which sector-department do you work in?	0,4%	1,3%	8,9%	34,2%	55,3%	100.0%

Table 10 Crosstabulation for Q7 and Q11

Crosstab (Q6*Q11)		**Q11. Do you shop on the internet at internet cafes?**					Total
		Certainly yes	Yes	Sometime s	No	Certainly no	
Q6. Do you work ?	Students / graduates (who answered as “No” in Q6)	1,0 %	5,1 %	7,2 %	40,2 %	46,4 %	100.0%

Table 11 Crosstabulation for Q6 and Q11

In Q11, the answers “No” and “Certainly no” are taken into consideration when evaluating in this question. More than % 80 of them find shopping at internet cafes insecure and do not shop at internet cafes. But more than 90 % of employees working in non-IT sector and IT department find shopping at internet cafes insecure that they are very awared of the situtation. It is also much more than the others (Table 10). It may be concluded that awareness level for all sample domains in this question is “satisfactory” and “very satisfactory” level. To remind the Chi-Square test value for Q11, respondents mostly are heavily concentrated on specific option (Table 1). The results of Q11 are also significant because all of the respondents in the groups have obviously marked “certainly no”.

Crosstab (Q7*Q12)			**Q12. Do you know about the filtering tools that prevent children from seeing unwanted contents on the Internet?**					Total
			Nothing	Very little	Average	Much	Very much	
Q7. Which sector-department do you work in?	IT sector and IT department	% within which sector-department do you work in?	5,4%	12,5%	28,6%	32,1%	21,4%	100.0%
	IT sector and non-IT department	% within which sector-department do you work in?	1,5%	16,4%	28,4%	28,4%	25,4%	100.0%
	Non-IT sector and IT department	% within which sector-department do you work in?	4,2%	14,6%	37,5%	33,3%	10,4%	100.0%
	Non-IT sector and non-IT department	% within which sector-department do you work in?	7,6%	30,8%	30,0%	21,9%	9,7%	100.0%

Table 12 Crosstabulation for Q7 and Q12

Crosstab (Q6*Q12)		**Q12. Do you know about the filtering tools that prevent children from seeing unwanted contents on the Internet?**					Total
		Nothing	Very little	Average	Much	Very much	
Q6. Do you work ?	Students / graduates (who answered as “No” in Q6)	9,3 %	34,0 %	33,0 %	17,5 %	6,2 %	100.0%

Table 13 Crosstabulation for Q7 and Q12

In Q12, average and above scales (“much” and “very much) can be thought that existence of certain ISA level is present in employees’ knowledge. The ratio of their knowledge (average and above) about filtering tools that prevent children from facing with unwanted harmful contents is more than 75 %. Employees reside in sample domain-B (SD-B) have more than 80 % as well as in SD-C while SD-D has at more than 60 %. SD-D have the average ISA level that is less than the others (Table 12). Regarding the results of the students in Q12, 34 % of them know very little about unwanted content filtering tools on the internet, which is unsatisfactory ISA level for our scale and 32 % of them have knowledge in moderate level (Table 13).

Variables	Subvariables	Frequency	Percent
Q13. Do you have a membership for any social media platform like Facebook, Twitter, Instagram and so on?	a. Yes b. No	477 28	94,5 5,5

Table 14 Frequency Analysis for Q13

From the distribution of Q13 rates, more than 90% of all of the participants have social media account (Facebook, Twitter, Instagram etc.) that it indicates that most of the participants may be subjected to security incidents in social. Therefore, they need to know how to act along with the code of conduct in social media. The rates of Q13 is also confirmed that only one option has highly chosen by all of the respondents.

Before evaluating the Q14, name, surname, picture, emotions, thoughts, hobbies and research/studies are primary data set and daily terms flowing over social media. Once you signed into social network, you absolutely share one of these data for subscription at least. On the other hand, there are some issues to know while sharing. Identification number, phone number and e-mail address are so unique that identify only one person all over the world. They are type of risky personal data to share. Moreover, it is so risky if we are using the pages whose privacy setting on public. Everyone can obtain those. To remind that social engineers collect these valuable data assets of people from social media.

Crosstab (Q14*Q7)		Q7. Which sector-department do you work in?			
		IT sector IT department	IT sector non- IT department	Non- IT sector IT department	Non-IT sector non- IT department
Q14.Which personal information that you mostly share in social media?	Picture	75,0 %	73,4 %	85,1 %	73,9%
	Video	28,8 %	21,9 %	51,1 %	23,3 %
	Name, surname	48,1 %	67,2 %	72,3 %	59,5 %
	Birthdate	23,1 %	34,4 %	19,1 %	30,7 %
	Name, surname of family members	1,9 %	7,8 %	6,4 %	8,8 %
	ID number	5,8 %	0 %	0 %	1,86 %
	Phone number	11,5 %	12,5 %	4,3 %	7,9 %
	E-mail address	38,5 %	45,3 %	61,7 %	35,8 %
	Research/ studies	26,9 %	20,3 %	17,0 %	18,1 %
	Emotions	40,4 %	42,2 %	38,3 %	28,4 %
	Thoughts	51,9 %	57,8 %	48,9 %	52,1 %
	Hobbies	%42,3	40,6 %	46,8 %	34,4 %
Total		100 %	100 %	100 %	100 %

Table 15 Crosstabulation for Q14 and Q7

Regarding the answers of 4 sample domains in Table 15, ID number, phone number and name of family members have been least shared personal data. It is supposed to be “satisfactory” in terms of IS concerns.

Picture is the most commonly shared type of data among all four of sample domains. No matter what we share, any combination of these data can result in being exposed to social engineering. It is better to customize privacy setting of personal pages as “on private” rather than “on public” if extensive type of personal data have been sharing.

Crosstab (Q14*Q6)		Q6. Do you work?
		Students / graduates (who answered as “No” in Q6)
Q14.Which personal information that you mostly share in social media?	Picture	73,6 %
	Video	24,2 %
	Name, surname	65,9 %
	Birthdate	30,8 %
	Name, surname of family members	12,1 %
	ID number	3,3 %
	Phone number	7,7 %
	E-mail address	45,0 %
	Research/ studies	22,0 %
	Emotions	30,8 %
	Thoughts	52,7 %
	Hobbies	35,2 %
Total		100 %

Table 16 Crosstabulation for Q14 and Q6

With regard to students/graduates- non-workers, more than 70 % of them have been mostly sharing pictures, name and surname and their thoughts in these social media networks with regard to Q14. Considering the IS concerns, sharing identity number and phone number at very slight amount is expected behaviour and perhaps, it may be evaluated as somehow mismarking (Table 16).

Crosstab (Q7*Q15)			Q15. Have you ever faced with negative incident about information security?		
			Yes	No	Total
Q7. Which sector-department do you work in?	IT sector and IT department	% within which sector-department do you work in?	22,2%	77,8%	100.0%
	IT sector and non-IT department	% within which sector-department do you work in?	13,6%	86,4%	100.0%
	Non-IT sector and IT department	% within which sector-department do you work in?	12,5%	87,5%	100.0%
	Non-IT sector and non-IT department	% within which sector-department do you work in?	20,5%	79,5%	100.0%

Table 17 Crosstabulation for Q15 and Q7

Crosstab (Q6*Q15)		Q15. Have you ever faced with negative incident about information security?		
		Yes	No	Total
Q6. Do you work ?	Students / graduates (who answered as "No" in Q6)	20,0%	80,0%	100.0 %

Table 18 Crosstabulation for Q15 and Q6

In Q15, more than three quarter of employees who belong to any sample domain have not faced with any security incident (Table 17). But if the distribution of the answers in Q16 is viewed, four over five of the employees do believe that they can face security incident anytime anywhere (Table 18). This finding shows the sensitiveness of all four type of the respondents against IS topic in a way. It is so pleasing that they have somehow common threat perception.

Crosstab (Q7*Q16)			Q16. Do you think that you will probably face with such incidents in the future?		
			Yes	No	Total
Q7. Which sector-department do you work in?	IT sector and IT department	% within which sector-department do you work in?	85,0%	15,0%	100.0%
	IT sector and non-IT department	% within which sector-department do you work in?	83,0%	17,0%	100.0%
	Non-IT sector and IT department	% within which sector-department do you work in?	85,4%	14,6%	100.0%
	Non-IT sector and non-IT department	% within which sector-department do you work in?	86,5%	13,5%	100.0%

Table 19 Crosstabulation for Q16 and Q7

Crosstab (Q6*Q16)		Q16. Have you ever faced with negative incident about information security?		
		Yes	No	Total
Q6. Do you work ?	Students / graduates (who answered as "No" in Q6)	79,7 %	20,0%	100.0 %

Table 20 Crosstabulation for Q16 and Q6

In Q15 and Q16, almost all of respondents in SD-E believe that they will probably experience security incidents in the future although they haven't faced with any.

(Table 19 and Table 20). This finding shows that they have satisfactory IS threat perception.

Crosstab **(Q7*Q17)**		**Q7. Which sector-department do you work in?**			
		IT sector IT department	IT sector non-IT department	Non-IT sector IT department	Non-IT sector non-IT department
Q17. You faced with a content in a social media/website that violate your personal rights. Where do you report?	My family and/or friend	7,9 %	6,0 %	17,5 %	18,3 %
	The nearest police department	10,5 %	6,0 %	10,0 %	15,7 %
	Relative website admin	**57,9 %**	**64,0 %**	**77,5 %**	**55,0 %**
	Internet Service Provider (ISP)	13,2 %	14,0 %	10,0 %	8,9 %
	Internet Information Report Center (TIB)	23,7 %	48,0 %	37,5 %	43,3 %
	Cyber Security Branch Office	**31,6 %**	**42,0 %**	**30,0 %**	**23,3 %**
	Prosecution Office	**57,9 %**	**60,0 %**	**67,5 %**	**62,8 %**
	I do not know where to report	18,4 %	10,0 %	17,5 %	12,8 %
	I do not report	2,6 %	4,0 %	2,5 %	0,6 %

Table 21 Crosstabulation for Q17 and Q7

In Q17, correct way of behaviour is to consult to “relative website admin”, “cyber security branch offices” affiliated to police department in the city you live and “prosecution offices” respectively.

In SD-A, more than half of the respondents (average) in this domain chose relative web site admin and prosecution office which are also correct but the rate of answering as “cyber security branch offices” remained low which is unsatisfactory. Employees who belong to SD-B chose relatively much more correct answers in comparison with SD-A but SD-B also remained low for consulting to “cyber security branch office”, which is lower than average ISA level. SD-C also remained unsatisfactory at consulting to “cyber security branch offices” but they chose much more correct answers in consulting to website admin and “prosecution offices”. Employees in SD-D have the lowest ISA level in this question compared to other sample domains excluding consulting to “prosecution office.” Most surprisingly, employees working in SD-A answers around 18 % as “I do not know where to report". Eventually, all four types of domains remain unsatisfactory about consulting to "cyber security branch offices" when they faced with a security incident violating their personal rights.

Crosstab **(Q6*Q17)**		**Q6. Do you work ?**
		Students/graduates (who answered as "No" in Q6) are evaluated
Q17. You faced with a content in a social media/website that violate your personal rights. Where do you report?	My family and/or friend	5,4 %
	The nearest police department	6,4 %
	Relative website admin	**38,7 %**
	Internet Service Provider (ISP)	11,8 %
	Internet Information Report Center (TIB)	37,6 %
	Cyber Security Branch Office	**23,7 %**
	Prosecution Office	**18,3 %**
	I do not know where to report	20,4 %
	I do not report	20,4 %

Table 22 Crosstabulation for Q17 and Q6

Regarding the respondents who are students/graduates in Table 22, they most commonly chose "relative website admin", "the Presidency of Telecommunication" and "Cyber Security Branch Offices". When ISA scale was considered, the ratio of the answers which lead to correct way of behaviour is at "unsatisfactory" level. Additionally, it may be thought that respondents in this domain who "do not know where to report" are slightly more than in other sample domains. However, students or fresh graduates do less know the authority in charge of concerning cyber crimes and violation of personal rights on the internet when their personal rights were violated.

Crosstab (Q7*Q18)		**Q7. Which sector-department do you work in?**			
		IT sector IT department	IT sector non-IT department	Non-IT sector IT department	Non-IT sector non-IT department
Q18.When you faced with a unwanted content (encourage/help suicide and prostitution, harmful drugs, gambling, nudity, sexual harassment and crimes against Atatürk etc.). Where do you report?	My family and/or friend	2,0 %	6,4 %	10,9 %	9,4 %
	The nearest police department	8,0 %	6,4 %	2,2 %	9,0 %
	Relative website admin	**44,0 %**	**38,7 %**	**60,9 %**	**36,8 %**
	Internet Service Provider (ISP)	14,0 %	14,5 %	10,9 %	10,8 %
	Internet Information Report Center (TIB)	**32,0 %**	**59,7 %**	**34,8 %**	**41,3 %**
	Cyber Security Branch Office	14,0 %	33,9 %	21,7 %	15,7 %
	Prosecution Office	**36,0 %**	**41,9 %**	**54,4 %**	**32,7 %**
	I do not know where to report	16,0 %	12,9 %	10,9 %	21,1 %
	I do not report	12,0 %	8,1 %	19,6 %	8,5 %

Table 23 Crosstabulation for Q18 and Q7

From the illustration of Q18 above, correct way of behaviour when you faced with the types of unwanted content is to consult to “relative website admin”, “Internet Information Report Center” affiliated to the Presidency of Telecommunication in Turkey (TİB) and “prosecution offices” (Table 23).

Crosstab (Q6*Q18)		**Q6. Do you work?**
		Students/graduates (who answered as “No” in Q6) are evaluated
Q17. You faced with a content in a social media/website that violate your personal rights. Where do you report?	My family and/or friend	21,5 %
	The nearest police department	15,0 %
	Relative website admin	**40,9 %**
	Internet Service Provider (ISP)	6,4 %
	Internet Information Report Center (TIB)	**34,4 %**
	Cyber Security Branch Office	31,2 %
	Prosecution Office	**31,2 %**
	I do not know where to report	23,7 %
	I do not report	8,6 %

Table 24 Crosstabulation for Q18 and Q6

Employees reside in SD-C has the highest score at consulting to “relative website admin” and “prosecution office” in comparison with SD-A, SD-B and SD-D. SD-B has only “average” awareness level about consulting to “Internet Information Report Center”. Once again there are employees working in non-IT sector and non-IT department do not know where to report these kinds of issues which is around 21 %. Any other rates in all four of sample domains are below the average awareness level which is “unsatisfactory”.

3.1.3 Analysis of e-mail security

In this section, frequency analysis and crosstabs were applied between sector-department which are items of Q7 and e-mail security questions.

Variables	Subvariables	Frequency	Percent
Q19. Do you use e-mail address?	a. Yes b. No	471 4	99,2 0,8

Table 25 Frequency analysis of Q19

With respect to frequency analysis of Q19 for all of the participants, almost all of them have been using e-mail addresses that the results of Q20 is significant on groups.

Crosstab (Q7*Q20)			Q20.What is SPAM?				Total
			SPAM is an antivirus solution	SPAM is a firewall	SPAM is an unwanted and mass e-mails	SPAM is an e-mail attachment	
Q7. Which sector-department do you work in?	IT sector and IT department	% within which sector-department do you work in?	4,3%	6,5%	89,1%	0 %	100.0%
	IT sector and non-IT department	% within which sector-department do you work in?	4,9%	6,6%	86,9%	1,6 %	100.0%
	Non-IT sector and IT department	% within which sector-department do you work in?	0 %	6,5%	91,3%	2,2 %	100.0%
	Non-IT sector and non-IT department	% within which sector-department do you work in?	1,9%	13,2%	79,2%	5,7%	100.0%

Table 26 Crosstabulation of Q20 and Q7

Crosstab (Q6*Q20)		**Q20.What is SPAM?**				
		SPAM is an antivirus solution	SPAM is a firewall	SPAM is an unwanted and mass e-mails	SPAM is an e-mail attachment	TOTAL
Q6. Do you work ?	Students / graduates (who answered as “No” in Q6)	2,33 %	10,5%	81,4 %	5,8 %	100.0 %

Table 27 Crosstabulation of Q20 and Q6

Regarding the crosstab of Q20, high ratio in having knowledge about SPAM attracts the attention at the first sight. All of the employees working in various sector and departments have “satisfactory” knowledge about what SPAM e-mail is at least (Table 26). Non-workers also have “satisfactory” knowledge about the term “SPAM” with 81,4 % (Table 27).

Crosstab (Q7*Q21)			**Q21.What do you do when you got an e-mail asking to update your personal info by clicking the link in the e-mail body?**				Total
			I click the link if logo and address of the bank is right	I do the same if my close friends update their info	**I make a call to bank to get information about the e-mail**	I do not have any idea	
Q7. Which sector-department do you work in?	IT sector and IT department	% within which sector-department do you work in?	19,6%	2,2%	**76,1%**	2,2 %	100.0%
	IT sector and non-IT department	% within which sector-department do you work in?	13,1%	1,6%	**80,3%**	4,9 %	100.0%
	Non-IT sector and IT department	% within which sector-department do you work in?	4,3 %	0 %	**89,1%**	6,5 %	100.0%
	Non-IT sector and non-IT department	% within which sector-department do you work in?	10,8%	0,5%	**78,3%**	10,4%	100.0%

Table 28 Crosstabulation of Q21 and Q7

In Q21, most of the employees in all 4 sample domains feel unsafe to update their personal records when they got an e-mail coming from alleged banks. More than

75% of them make a call to their bank to get more accurate information to confirm the e-mail source. ISA level of all of the internet users in this question is “satisfactory” and above (Table 28).

Crosstab (Q6*Q21)		Q21.What do you do when you got an e-mail asking to update your personal info by clicking the link in the e-mail body?				
		I click the link if logo and address of the bank is right	I do the same if my close friends update their info	**I make a call to bank to get information about the e-mail**	I do not have any idea	TOTAL
Q6. Do you work ?	Students / graduates (who answered as “No” in Q6)	2,33 %	10,5%	**81,4 %**	5,8 %	100.0 %

Table 29 Crosstabulation of Q21 and Q6

From the perspective of students/graduates who are non-workers, they also find unsafe to click on the link within the e-mail body. They present satisfactorily correct way of behaviour in such situation with respect to IS principal (Table 29).

Crosstab (Q7*Q22)			Q22.What do you do when you got an e-mail saying that a little girl is lost for a while and ask you to forward the e-mail as many people as you can?				Total
			I forward to all of my contacts	I forward to closest contacts	**I create a new post to ask sender not to forward chain e-mail**	I do not have any idea	
Q7. Which sector-department do you work in?	IT sector and IT department	% within which sector-department do you work in?	13,0%	13,0%	**52,2%**	21,7 %	100.0%
	IT sector and non-IT department	% within which sector-department do you work in?	4,9%	6,6%	**59,0%**	29,5 %	100.0%
	Non-IT sector and IT department	% within which sector-department do you work in?	4,3 %	6,5 %	**76,1%**	13,0 %	100.0%
	Non-IT sector and non-IT department	% within which sector-department do you work in?	13,7%	11,8%	**36,8%**	37,7%	100.0%

Table 30 Crosstabulation of Q22 and Q7

Crosstab (Q6*Q22)		Q22. What do you do when you got an e-mail from your friend but file extension of the attachment and domain name of the address (the section after ‘@’ sign) is weird?				Total
		I forward to all of my contacts	. I forward to closest contacts	**I create a new post to ask sender not to forward chain e-mail**	I do not have any idea	
Q6. Do you work?	Students / graduates (who answered as “No” in Q6)	12,8 %	10,5 %	**34,9 %**	41,9 %	100.0%

Table 31 Crosstabulation of Q22 and Q6

In Q22, employees in SD-A have chosen correct answer which is 52,2 % and equivalent to “average” ISA level as well as SD-B has. Employees who reside in SD-C have the highest score compared to other employees who reside in other sample domains, which is “satisfactory” ISA level. Employees working in non-IT sector and non- IT department (SD-D) has the lowest score, which is graded as “unsatisfactory” ISA level. Besides they have chosen mainly “I do not have any idea” option (Table 30). Most surprisingly, this finding shows that SD-D will probably be vulnerable to fishing attacks by e-mail as well as students/graduates (Table 31).

Crosstab (Q7*Q23)			Q23. What do you do when you got an e-mail from your friend but file extension of the attachment and domain name of the address (the section after ‘@’ sign) is weird?				Total
			It is safe to open up attach as the sender is friend of mine.	I reply to e-mail to confirm if it is really sent by my friend	**I create new post to send to my friend’s address in my contact for confirmation**	I do not have any idea	
Q7. Which sector-department do you work in?	IT sector and IT department	% within which sector-department do you work in?	4,3%	15,2%	**60,9%**	19,6%	100.0%
	IT sector and non-IT department	% within which sector-department do you work in?	0,0%	23,0%	**54,1%**	23,0%	100.0%
	Non-IT sector and IT department	% within which sector-department do you work in?	2,2%	23,9%	**60,9%**	13,0%	100.0%
	Non-IT sector and non-IT department	% within which sector-department do you work in?	2,4%	27,4%	**38,2%**	32,1%	100.0%

Table 32 Crosstabulation of Q22 and Q7

54. 1 % of the employees in IT sector and non-IT department (SD-B) that they do not trust the e-mails coming from a friend and having attachments with weird file extensions and domain name of the e-mail address which is after the '@' sign. ISA level for this sample domain is "average" (Table 32). 60.9 % of employees in IT sector and IT department (SD-A) answered correctly to this question, which is "average" ISA level as well as in SD-C (Table 32).

Only 38,2 % of employees who work in non-IT sector and IT department (SD-D) performed correct way of behaviour against such situation. The ratio of ISA level stay considerably lower than the others, which is equivalent to "unsatisfactory level" (Table 32). According to Table 1 as mentioned earlier, shown that respondants in all groups have chosen unique option "I create new post to send to my friend's address in my contact for confirmation" so that the results of Q23 on five sample domains are statistically significant.

Crosstab (Q7*Q23)		**Q23. What do you do when you got an e-mail from your friend but file extension of the attachment and domain name of the address (the section after '@' sign) is weird?**				Total
		It is safe to open up attach as the sender is friend of mine.	I reply to e-mail to confirm if it is really sent by my friend	**I create new post to send to my friend's address in my contact for confirmation**	I do not have any idea	
Q6. Do you work?	Students / graduates (who answered as "No" in Q6)	5,8 %	29,1 %	**43,0 %**	22,1 %	100.0%

Table 33 Crosstabulation of Q23 and Q6

Students/graduates who are non-workers and reside in SD-E stay below the "average" ISA level for this question (Table 33).

3.1.4 Analysis of safely use of internet and computer

Crosstab (Q7*Q24)		Q7. Which sector-department do you work in?			
		IT sector and IT department	IT sector and non-IT department	Non-IT sector and IT department	Non-IT sector and non-IT department
Q24. Which countermeasures do you take in case your laptop is stolen?	Keep its physical (MAC) address	39,6 %	37,3 %	10,9 %	14,6 %
	Keep its serial number	50,0 %	40,7 %	47,8 %	32,0 %
	Backup my sensitive data	50,0 %	35,6 %	54,3 %	33,0 %
	Encrypt my sensitive data	68,7 %	64,4 %	80,4 %	66,5 %
	Install an alarm software	10,4 %	3,4 %	6,5 %	4,8 %
	Set passwords for my user accounts	50,0 %	49,1 %	58,7 %	46,6 %
	Mark a sign to an unrecognizable place on my laptop	8,3 %	1,7 %	17, 4 %	2,4 %
	Install a GPS software to trace remotely	35,4 %	30,5 %	15,2 %	18,4 %

Table 34 Crosstabulation of Q24 and Q7

Crosstab (Q6*Q24)		Q6. Do you work?	Total Response (for each option)
		Students / graduates (who answered as "No" in Q6)	
Q24. Which countermeasures do you take in case your laptop is stolen?	Keep its physical (MAC) address	24,1 %	100 %
	Keep its serial number	34,5 %	100 %
	Backup my sensitive data	32,2 %	100 %
	Encrypt my sensitive data	57,5 %	100 %
	Install an alarm software	5,7 %	100 %
	Set passwords for my user accounts	46,0 %	100 %
	Mark a sign to an unrecognizable place on my laptop	5,7 %	100 %
	Install a GPS software to trace remotely	23,0 %	100 %

Table 35 Crosstabulation of Q24 and Q6

Q24 evaluates the precautions that respondents could take in case their laptops are somewhat stolen. There are 8 precautions that are all correct but first two of them are highly important to find a stolen laptop: keeping serial number and physical MAC address.

From the observation in Table 34, it is indicated that all of the respondents in five sample domains often seek for “encrypting sensitive data” in case their laptops are stolen despite this is not the first thing to do. The first thing is to note down the serial number and physical address of the laptop a separate safe place to find easily lately.

68 % of employees in SD-A, which makes “average” ISA level, are mostly interested in “encrypting sensitive data” against being stolen as well as other domains. 50 % of employees in SD-A take care of “keeping their laptop serial number”, “backing up their sensitive data” and “setting passwords for user accounts” in case laptop is stolen, which is “average” level. But answering as “keeping MAC address” is at “unsatisfactory” ISA level that it is so annoying in terms of IT sector and IT department domain. All other precautions are preferred at degree of “unsatisfactory” and “very unsatisfactory”.

Employees in SD-B have the similar ISA level with SD-A for all precautions excluding the “keeping its serial number” and “backing up sensitive data”, which are at “unsatisfactory” levels.

Employees in SD-C have “satisfactory” ISA level in “encrypting sensitive data”, which is the highest ISA level among all five domains. The first two options incase being stolen: “keeping MAC address” (10, 9 %- “very unsatisfactory) and “keeping serial number” (47,8 %, “average”) respectively.

Despite the fact that SD-D has the highest distribution (number of participants), employees in SD-D have “very unsatisfactory” level in “keeping MAC address” and “unsatisfactory” level in “keeping serial number” of the laptop in case it is stolen.

On the other hand, students are unawared of “keeping MAC address” and “keeping serial number” in case laptop is stolen, which are both at “unsatisfactory” ISA levels. Students are “averagely” awared of “encrypting sensitive data” and “setting password for user accounts” which are as same as in other domains (Table 35).

Crosstab (Q7*Q25)		Q7. Which sector-department do you work in?			
		IT sector and IT department	IT sector and non-IT department	Non-IT sector and IT department	Non-IT sector and non-IT department
Q25. Do you activate screen saver with password when you took a little break to return in the middle of your studies?	I only activate in my business laptop	25 %	27,1 %	47,8 %	32,0 %
	I only activate in my personal computer	0 %	6,8 %	2,2 %	5,8 %
	I use it in both	60,4 %	49,1 %	32,6 %	25,7 %
	I do not activate as I go back to work in short time	10,4 %	6,8 %	6,5 %	10,2 %
	I do not activate as my data is not that critical	4,2 %	10,2 %	10,9 %	26,2 %
Total responses		100 %	100 %	100 %	100 %

Table 36 Crosstabulation of Q25 and Q7

Crosstab (Q6*Q25)		Q6. Do you work?	Total responses
		Students / graduates (who answered as “No” in Q6)	
Q25. Do you activate screen saver with password when you took a little break to return in the middle of your studies?	I only activate in my business laptop	10,3 %	100 %
	I only activate in my personal computer	6,9 %	100 %
	I use it in both	40,2 %	100 %
	I do not activate as I go back to work in short time	16,1 %	100 %
	I do not activate as my data is not that critical	26,4 %	100 %

Table 37 Crosstabulation of Q25 and Q6

Q25 focuses on use of password protected screen saver in operating systems. The correct way of behaviour in this question is to use screen saver with password protection in both personal and business computers even if we will go back in a minute in business environment or even we are alone at home, that is, there is no one to physically access to computer, or even more if data we stored is not much critical. This is just a way of developing a proper security habit before gaining it as behaviour.

In this respect, we can't say that there is an optimistic result from the observations of the illustration above (Table 36 and Table 37). Only employees SD-A and SD-B take care of using password protected screen saver in both environments, which are at "average" ISA level. All the others remain below the average because they have occasionally checked as their data is not critical or they use it only in business environments.

Crosstab (Q7*Q26)		**Q7. Which sector-department do you work in?**			
		IT sector and IT department	IT sector and non-IT department	Non-IT sector and IT department	Non-IT sector and non-IT department
Q26. How do you distinguish if a website is a safe to surf or not?	Websites that offer freeware are safe	2,2 %	0 %	0 %	0 %
	Online casinos are safe	0 %	0 %	2,2 %	0 %
	It is safe if a security logo exists	21,7 %	19,3 %	17,4 %	24,4 %
	It is safe if the web browser shows small gold lockpad	**54,3 %**	**56,1 %**	**67,4 %**	**42,8 %**
	It is safe if its address starts with "https://" instead of "http://"	**65,2 %**	**68,4 %**	**73,9 %**	**38,3 %**
	It is safe if it appears to be popular	6,5 %	8,8 %	8,7 %	6,5 %
	I am having difficulty in distinguishing	23,9 %	21,0 %	17,4 %	49,2 %
Total responses		100 %	100 %	100 %	100 %

Table 38 Crosstabulation of Q26 and Q7

Q26 evaluates the knowledge of respondents about safe website concept to surf confidently. There are two options that are correct marked as bold. Employees in SD-A, SD-B and SD-C stay at "average" ISA level concerning with small golden lockpad generall appeared inside address bar in the web browsers while SD-D and SD-E remain below the average which is "unsatisfactory". Why SD-D and SD-E have far less awareness in this topic is because they mostly have been having difficulty in distinguishing safe and unsafe websites which is so surprising finding that it should be ruminated on (Table 38 and 39). Even if there is a slight peak at other option "it is safe if website starts with 'https' instead of 'http'", employees in

SD-D are again at “unsatisfactory” ISA level. In this option, students have much more knowledge (“average”) even if they are represented low in numbers (Table 39).

Crosstab (Q6*Q26)		**Q6. Do you work?**	Total responses
		Students / graduates (who answered as “No” in Q6)	
Q26. How do you distinguish if a website is a safe to surf or not?	Websites that offer freeware are safe	2,3 %	100 %
	Online casinos are safe	2,3 %	100 %
	It is safe if a security logo exists	20,0 %	100 %
	It is safe if the web browser shows small gold lockpad	**43,5 %**	**100 %**
	It is safe if its address starts with “https://” instead of “http://”	**50,6 %**	**100 %**
	It is safe if it appears to be popular	7,1 %	100 %
	I am having difficulty in distinguishing	29,4 %	100 %

Table 39 Crossabulation of Q26 and Q6

Q27 focuses on how far the respondents take ADSL security measures. At first sight, “setting a wireless password” is the unique option raising high for all five of sample domains. In this respect, we can conclude that most of the respondents know about setting a wireless password for their modems. On the other hand, encrypting communication with these wireless password shouldn’t have so much mattered to SD-A, SD-B, SD-D and SD-E that it appears to be dropping at rate with regard to “setting a wireless password”. Nevertheless, shown that all of the sample domains have “average” and above ISA level with regard to WPA/WPA2 encryption in modem security settings apart from the employees in SD-D, which is at “unsatisfactory” ISA level. Setting a password for web interface of modem is the second important security measure that employees in SD-A, SD-B and SD-C are good at but SD-E and SD-D.

Crosstab (Q7*Q27)		**Q27. Which security measures below do you take in your ADSL modem?**			
		IT sector and IT department	IT sector and non-IT department	Non-IT sector and IT department	Non-IT sector and non-IT department
Q7. Which sector-department do you work in?	Shut down my modem when I do not use it	39,1 %	29,8 %	15,2 %	36,1 %
	Set a password for web interface	58,7 %	56,1 %	67,4 %	33,7 %
	Set a wireless connection password	65,2 %	78,9 %	76,1 %	73,3 %
	Encrypt connection between computer and modem via WPA/WPA2	56,5 %	59,6 %	73,9 %	32,7 %
	Prevent SSID broadcast	26,1 %	24,6 %	30,4 %	9,4 %
	Shut down unused and unnecessary services	26,1%	17,5 %	34,8 %	8,9 %
	Activate modem firewall	37,0 %	36,8 %	41,3 %	26,7 %
	Filter MAC address(es)	21,7 %	35,1 %	30,4 %	8,4 %
	Check modem firmware updates	28,3 %	26,3 %	37,0 %	15,8 %
Total responses		100 %	100 %	100 %	100 %

Table 40 Crosstabulation of Q27 and Q7

Even if the rates of almost all of the security measures raised high for SD-C in comparison with the other sample domains, they are all at insufficient ISA level, which is below “average”, is far from the appropriate level of security means. In addition, even if a user doesn’t want to restrict access to modem only for specific persons whose MAC address on filtering list (say it depends on user need), the others which are basic security practices of ADSL modem in this question may be applied in proper fashion.

Crosstab (Q6*Q27)		Q6. Do you work?	Total responses
		Students / graduates (who answered as “No” in Q6)	
Q27. Which security measures below do you take in your ADSL modem?	Shut down my modem when I do not use it	32,9 %	100 %
	Set a password for web interface	35,3 %	100 %
	Set a wireless connection password	64,7 %	100 %
	Encrypt connection between computer and modem via WPA/WPA2	40,0 %	100 %
	Prevent SSID broadcast	14,1 %	100 %
	Shut down unused and unnecessary services	11,8 %	100 %
	Activate modem firewall	22,3 %	100 %
	Filter MAC address(es)	16,5 %	100 %
	Check modem firmware updates	14,1 %	100 %

Table 41 Crosstabulation of Q27 and Q6

3.1.5 Analysis of threats and preventive measures

Q28 and Q29 concern with use of peer-to-peer file sharing software and the threats they exposed. In Q28, respondents who have answered as “Yes” and “No” differ at population. That’s why addition of all the total responses make 544- the total participants who joined the survey.

Crosstab (Q7*Q28)			Q28.Have you ever used peer-to-peer file sharing software like Kazaa, LimeWire, uTorrent, eMule and so on?		
			Yes	No	TOTAL
Q7. Which sector-department do you work in?	IT sector and IT department	% within which sector-department do you work in?	68,9%	31,1%	100.0%
	IT sector and non-IT department	% within which sector-department do you work in?	75,4%	24,6%	100.0%
	Non-IT sector and IT department	% within which sector-department do you work in?	74,4%	25,6%	100.0%
	Non-IT sector and non-IT department	% within which sector-department do you work in?	41,1%	58,9%	100.0%

Table 42 Crosstabulation for Q28 and Q7

Crosstab (Q7*Q28)		Q28.Have you ever used peer-to-peer file sharing software like Kazaa, LimeWire, uTorrent, eMule and so on?		Total
		Yes	No	
Q6. Do you work?	Students / graduates (who answered as "No" in Q6)	61,2 %	38,8 %	100.0%

Table 43 Crosstabulation of Q28 and Q6

Employees in SD-D have much tendency towards answering "No" while others are exactly opposing the same answer as well as students/graduates (Table 42 and 43). It can be obtained that most of the respondents use file sharing software excluding the workers in non-IT sector and non- IT departments in this survey. Shown that Q28 is significant on 5 sample domains according to responses that the respondants made that all five groups have been using p2p file sharing software.

Crosstab (Q7*Q29)			Q29.Which ones are the threats originated by peer-to-peer file sharing software?			
			I may violate copyright of music, video or any other software	**The program I downloaded may include malicious software**	**I may allow bad guys with bad intentions to see my personal data**	**Total Responses**
Q7. Which sector-department do you work in?	IT sector and IT department	% within which sector-department do you work in?	**55,2%** **16**	**79,3%** **23**	**65,5 %** **19**	29
	IT sector and non-IT department	% within which sector-department do you work in?	**78,0%** **32**	**87,8%** **36**	**68,3%** **28**	41
	Non-IT sector and IT department	% within which sector-department do you work in?	**43,7%** **14**	**87,5%** **28**	**68.7%** **22**	32
	Non-IT sector and non-IT department	% within which sector-department do you work in?	**66,7%** **54**	**81,5%** **66**	**82.7%** **67**	81

Table 44 Crosstabulation for Q29 and Q7

Q29 is composed of three options to pick, which are all of them are correct statements about file sharing software, and can be checked by the respondents because there is a question rule for Q29 that a participant can check 3 options at most. As mentioned earlier, each option is evaluated over 100% in these kinds of questions that enable participants check more than one option; however, each option will be considered accordingly.

Crosstab (Q6*Q29)		Q29.Which ones are the threats originated by peer-to-peer file sharing software?			Total responses
		I may violate copyright of music, video or any other software	The program I downloaded may include malicious software	I may allow bad guys with bad intentions to see my personal data	
Q6. Do you work?	Students / graduates (who answered as “No” in Q6)	54,9 % 28	78,4 % 40	64,7 % 33	51

Table 45 Crosstabulation of Q29 and Q6

In Table 44, respondents who reside in SD-A mostly suppose that a file type downloaded via file sharing software can be infectious as well as SD-B and SD-C think that way. By using p2p file sharing software, you open folders which you want to share to public. The respondents from SD-D are mostly awared of this situation which is at 82.7%. By downloading a music file, video or any kind of digital material of one of copyright owner, we can violate copyright laws and permissions. Employees who belong to SD-D are much more awared of this matter, which is 66, 7% at rate. The numbers just below the percentages stand for how many times the respondents picked up the option. The numbers in total column stand for total respondents who answered to the question from that sample domain.

On the other hand, if all of the answers are correct, there is more important question arised that how many respondents exactly picked up all of three correct options. After each correct option was filtered to see how many people have only chosen specific option and was applied to AND operation, only 108 people answered correctly from 254 responses in total for all of the sample domains, which makes roughly 42% and “unsatisfactory”. 11 employees out of 29 from IT sector and IT department (SD-A), 23 employees out of 41 from IT sector and non-IT department (SD-B), 14 employees out of 32 from non-IT sector and IT department (SD-C), 41 employees out of 81 from non-IT sector and non-IT department (SD-D) and 19 students/graduates out of 51 respondents (SD-E) are awared of all three of the threats exposed by using p2p file sharing software, however, the equivalent ISA level of these sample domains were calculated by dividing the number of respondents who checked all three of the selections to number of total respondents in each sample domain. They are estimated respectively as follows: 37,9% (11/29), 56,0% (23/41), 43,7% (14/32), 50,6% (41/81) and 37,2% (19/51), thereby all sample domains reside in "unsatisfactory" ISA level for knowing risks of using p2p software excluding SD-B, and SD-D which are at "average".

Crosstab (Q7*Q30)			**Q30.What do you think about updates of your types of software installed in your computer?**				Total
			I install at once if there is available update	I install few days later after I take care of my other tasks	I get help from my closest friends	I do not have any idea	
Q7. Which sector-department do you work in?	IT sector and IT department	% within which sector-department do you work in?	**71,4%**	21,4%	7,1%	0,0%	100.0%
	IT sector and non-IT department	% within which sector-department do you work in?	**61,8%**	27,3%	5,5%	5,5%	100.0%
	Non-IT sector and IT department	% within which sector-department do you work in?	**72,1%**	20,9%	4,7%	2,3%	100.0%
	Non-IT sector and non-IT department	% within which sector-department do you work in?	**44,2%**	28,1%	20,1%	7,5%	100.0%

Table 46 Crosstabulation of Q30 and Q7

Q30 tests respondents' behaviour against updating software installed in the computer. Although all of four sample domains seem to be on time when they got an available update in their computers but SD-D is slightly below the average ISA level, 45 %. Nevertheless, it is accepted as "unsatisfactory". Once again the results of Q30 is significant on all five groups as well.

Crosstab (Q6*Q30)		Q30.What do you think about updates of your types of software installed in your computer?				Total
		I install at once if there is available update	I install few days later after I take care of my other tasks	I get help from my closest friends	I do not have any idea	
Q6. Do you work?	Students / graduates (who answered as "No" in Q6)	**49,4 %**	33,7 %	13,2 %	3,6 %	100.0%

Table 47 Crosstabulation of Q30 and Q6

In other words, why they pay less attention to updating on time is because they have much tendency towards preferring completion of other tasks in the computer to updating software, which is much more common behaviour displayed by students. Most notably, employees in SD-D have been seeking advises of their friends about software updates more than any others may be caused by the distribution of the respondents in high number. SD-A and SD-C take care of updating satisfactorily while SD-B seems to be averagely careful in ISA level.

Crosstab (Q7*Q31)			Q31. What type of antivirus software do you use in your computer?					Total
			I use free antivirus software	I use cracked antivirus software	I use license paid antivirus software	I do not use antivirus software	I do not have any idea	
Q7. Which sector-department do you work in?	IT sector and IT department	% within which sector-department do you work in?	35,7%	4,8%	54,8%	4,8%	0 %	100.0%
	IT sector and non-IT department	% within which sector-department do you work in?	41,8%	14,5%	34,5%	7,3%	1,8 %	100.0%
	Non-IT sector and IT department	% within which sector-department do you work in?	41,9%	7,0%	46,5%	4,7%	0 %	100.0%
	Non-IT sector and non-IT department	% within which sector-department do you work in?	37,7%	5,5%	42,7%	12,1%	2,0 %	100.0%

Table 48 Crosstabulation of Q31 and Q7

Crosstab (Q6*Q31)		**Q31. What type of antivirus software do you use in your computer?**					Total
		I use free antivirus software	I use cracked antivirus software	I use license paid antivirus software	I do not use antivirus software	I do not have any idea	
Q6. Do you work?	Students / graduates (who answered as “No” in Q6)	39,8 %	13,2 %	25,3 %	16,9 %	4,8 %	100.0%

Table 49 Crosstabulation of Q31 and Q6

In Q31, there isn’t only one certain correct option to choose because people are free to use free antivirus software as well as licensed or cracked antivirus software. Besides that, there are absolutely some differences among them. We can not redirect people to buy a licensed one which would be inconvenient in ethical terms but it is necessary to put the differences to tailor their needs because new emerging threats are always present in front of the door by evolving everyday.

Antivirus software protects computer viruses by signatures. When we get an update, it may be thought that new signatures are up. When we buy new antivirus software, we actually buy a signature database in broader terms; however, no one can expect the same signature database for free. In other words, most types of free antivirus software do not provide full protection. They commonly come with features to scan hard-drives and external drives while licensed ones are able to provide full protection like antispam filtering, identifying unsafe phishing websites, and malware and firewall protection. As for the cracked antivirus software, too few of them are free of trojans or backdoors. Most of them can be installed in some websites/forums providing free various types of software and utilities. In this regard, using licensed software seems to be more favorable. We observe that employees in SD-A pay attention to use licensed antivirus software more than other domains. Only employees in SD-B much more take care of using free antivirus. According to ISA level grading, SD-A and SD-C are “average” while SD-B, SD-D and SD-E are “unsatisfactory”.

Crosstab (Q7*Q32)			**Q32. How often do you make security scanning in your computer?**					Total
			Never	Rare	Average	Often	Very often	
Q7. Which sector-department do you work in?	IT sector and IT department	% within which sector-department do you work in?	5,0%	7,5%	47,5%	22,5%	17,5 %	100.0%
	IT sector and non-IT department	% within which sector-department do you work in?	7,8%	15,7%	47,1%	17,6%	11,8 %	100.0%
	Non-IT sector and IT department	% within which sector-department do you work in?	0 %	12,2 %	48,8%	34,1%	4,9 %	100.0%
	Non-IT sector and non-IT department	% within which sector-department do you work in?	6,3%	20,6%	40,0%	29,1%	4,0 %	100.0%

Table 50 Crosstabulation of Q32 and Q7

Crosstab (Q6*Q32)		**Q32. How often do you make security scanning in your computer?**					Total
		Never	Rare	Average	Often	Very often	
Q6. Do you work?	Students / graduates (who answered as “No” in Q6)	13,2 %	22,1 %	32,3 %	25,0 %	7,3 %	100.0%

Table 51 Crosstabulation of Q32 and Q6

Q32 concerns with the habit of the respondents of making security scanning in the computers. All four of employees in sample domains and students in SD-E have been making security scanning “averagely and above” against suspicious activities in the computers. The results of Q32 are significant as well.

Crosstab (Q7*Q33)			**Q33. How often do you backup your data in your computer?**					Total
			Never	Rare	Average	Often	Very often	
Q7. Which sector-department do you work in?	IT sector and IT department	% within which sector-department do you work in?	2,4%	11,9%	45,2%	28,6%	11,9 %	100.0%
	IT sector and non-IT department	% within which sector-department do you work in?	3,6%	14,5%	45,5%	21,8%	14,5 %	100.0%
	Non-IT sector and IT department	% within which sector-department do you work in?	4,7 %	9,3 %	62,8%	20,9%	2,3 %	100.0%
	Non-IT sector and non-IT department	% within which sector-department do you work in?	4,5%	18,6%	44,2%	23,6%	9,0 %	100.0%

Table 52 Crosstabulation of Q33 and Q7

Crosstab (Q6*Q33)		**Q33. How often do you backup your data in your computer?**					Total
		Never	Rare	Average	Often	Very often	
Q6. Do you work?	Students / graduates (who answered as “No” in Q6)	4,9 %	26,8 %	45,1 %	19,5 %	3,7 %	100.0%

Table 53 Crosstabulation of Q33 and Q6

In Q33, the habits of respondents of backing up their data assets are measured. We may notice from the observation of the table that all of the participants in all five sample domains have been giving importance to backing up their data assets in “average and above” ISA levels. The results of Q33 obviously significant.

Crosstab (Q7*Q34)			**Q34.Which one of the statements below is true?**				Total
			Only firewall is sufficient in a computer	Only antivirus software is sufficient in a computer	Both antivirus software and firewall perform same functionalities	**Both antivirus software and firewall need to be used updated in a computer**	
Q7. Which sector-department do you work in?	IT sector and IT department	% within which sector-department do you work in?	0 %	4,8 %	4,8%	**90,5%**	100.0%
	IT sector and non-IT department	% within which sector-department do you work in?	1,8%	3,6%	3,6%	**90,9%**	100.0%
	Non-IT sector and IT department	% within which sector-department do you work in?	4,7 %	7,0 %	9,3%	**79,1%**	100.0%
	Non-IT sector and non-IT department	% within which sector-department do you work in?	3,5%	4,0%	5,0%	**87,4%**	100.0%

Table 54 Crosstabulation of Q34 and Q7

In Q34, respondents are asked if they know the necessity of firewall and antivirus software together to provide full protection in a computer system. It can be concluded that all of the respondents from all five sample domains have "satisfactory" knowledge. The correct option has chosen by all of the respondants at significantly amount.

Crosstab (Q6*Q34)		**Q34.Which one of the statements below is true?**				Total
		Only firewall is sufficient in a computer	Only antivirus software is sufficient in a computer	Both antivirus software and firewall perform same functionalities	**Both antivirus software and firewall need to be used updated in a computer**	
Q6. Do you work?	Students / graduates (who answered as "No" in Q6)	4,9 %	4,9 %	8,5 %	**81,7 %**	100.0%

Table 55 Crosstabulation of Q34 and Q6

3.1.6 Analysis of Password Management and Security

Crosstab (Q7*Q35)			**Q35. What do you think about changing your passwords?**				Total Response (for each option)
			I change my password only if I doubt that somebody stole it	Changing process is boring	**I change my password regularly**	I change my password only if I have to give my friend	
Q7. Which sector-department do you work in?	IT sector and IT department	% within which sector-department do you work in?	**54,8 %**	4,8 %	**64,3%**	26,2%	100 %
	IT sector and non-IT department	% within which sector-department do you work in?	**60,0%**	20,0%	**40,0%**	36,4%	100 %
	Non-IT sector and IT department	% within which sector-department do you work in?	**75,0 %**	11,4 %	**25,0%**	38,6%	100 %
	Non-IT sector and non-IT department	% within which sector-department do you work in?	**52,8%**	18,3%	**41,6%**	27,4%	100 %

Table 56 Crosstabulation of Q35 and Q7

Crosstab (Q6*Q35)		**Q35. What do you think about changing your passwords?**				Total Response (for each option)
		I change my password only if I doubt that somebody stole it	Changing process is boring	**I change my password regularly**	I change my password only if I have to give my friend	
Q6. Do you work?	Students / graduates (who answered as “No” in Q6)	**63,7 %**	16,2 %	**27,5 %**	38,7 %	100 %

Table 57 Crosstabulation of Q35 and Q6

Q35 evaluates the password changing habits of respondents. There are two correct way of behaviour in this question that if a respondent changes his/her password at regular intervals and take care of changing when any suspicious activity arises, they exhibit correct way of behavior. The rest of two options are the usual user opinions that we are very familiar. Employees in SD-A “averagely” change their passwords regularly or seek for changing when they suspect that somebody take control of the account by stealing credentials. Employees in SD-B averagely change their passwords when they are suspicious against any stealing activity. They far less change passwords regularly, which is at "unsatisfactory" ISA level. Employees in SD-C have the highest ISA level when it comes to "changing passwords if they doubt somebody stole it", which is "satisfactory" ISA level. Contrary to the high level in this option, they "unsatisfactorily" change their passwords regularly. Employees in SD-D "averagely" change their passwords when they suspect while they are "unsatisfactory" in changing regularly as well as students/graduates in SD-E presented similar way of behaviour (Table 56 and Table 57).

Crosstab (Q7*Q36)		**Q36. How do you set your password?**			
		IT sector and IT department	IT sector and non-IT department	Non-IT sector and IT department	Non-IT sector and non-IT department
Q7. Which sector-department do you work in?	I use the password preset by the system	2,4 %	0 %	2,3%	2,6%
	I set short password not to forget	11,9%	20,0%	11,4%	15,9%
	I set all of my passwords same not to forget	14,3 %	16,4 %	18,2%	30,3%
	I set my password including upper, lower letters, numbers and special characters	76,2%	76,4%	77,3%	63,6%
	I set my passwords with 16 characters at least if the system allows	45,2 %	34,5 %	59,1 %	34,4 %
	I use password generator tool	0 %	7,3 %	6,8 %	3,6 %
Total response (for each option)		100 %	100 %	100 %	100 %

Table 58 Crosstabulation of Q36 and Q7

Q36 has an interest in how respondents set their passwords. Three of the options are correct way of behaviour while the rest comprises common incorrect way of behaviour made by most of the users unconsciously or insistently such as "using passwords preset by the system", "shortest passwords not to forget" and more dramatically "using same passwords for all accounts."

Employees in all four of sample domains "satisfactorily" form their passwords with the combination of upper, lower letters, numbers and special characters as well as students do. But they do not satisfactorily set their passwords with 16 characters even if the system allows. Rates are decreasing when it comes to setting passwords 16 characters long for all five of sample domains.

Crosstab **(Q6*Q36)**		**Q6. Do you work?**	Total Response (for each option)
		Students / graduates (who answered as “No” in Q6)	
Q36. How do you set your password?	I use the password preset by the system	1,2 %	100 %
	I set short password not to forget	19,7 %	100 %
	I set all of my passwords same not to forget	33,3 %	100 %
	I set my password including upper, lower letters, numbers and special characters	66,7 %	100 %
	I set my passwords with 8 characters at least if the system allows	24,7 %	100 %
	I use password generator tool	1,2 %	100 %

Table 59 Crosstabulation of Q36 and Q6

Only employees in SD-A and SD-C set passwords 16 characters long at “average” ISA levels while SD-B and SD-D are at “unsatisfactory” levels. Regarding the option “password generation tools”, almost none of the respondents seek for password generation software that has the capability to generate strong and steady passwords.

Crosstab (Q7*Q37)			**Q37. Who do you share your computer's authentication password with?**				Total
			I share with my trusted friend	I share with my trusted relative	I share with IT division in my institution	**I do not share with anyone**	
Q7. Which sector-department do you work in?	IT sector and IT department	% within which sector-department do you work in?	19,0 %	2,4 %	2,4%	**76,2%**	100 %
	IT sector and non-IT department	% within which sector-department do you work in?	12,7%	10,9%	5,5%	**70,9%**	100 %
	Non-IT sector and IT department	% within which sector-department do you work in?	34,9 %	4,7 %	9,3%	**51,2%**	100 %
	Non-IT sector and non-IT department	% within which sector-department do you work in?	17,3%	11,7%	10,7%	**60,4%**	100 %

Table 60 Crosstabulation of Q37 and Q7

Crosstab (Q6*Q37)		**Q37. Who do you share your computer's authentication password with?**				Total
		I share with my trusted friend	I share with my trusted relative	I share with IT division in my institution	**I do not share with anyone**	
Q6. Do you work?	Students / graduates (who answered as "No" in Q6)	25,6 %	15,8 %	2,4 %	**56,1 %**	100.0%

Table 61 Crosstabulation of Q37 and Q6

Q37 concerns with password sharing which can sound weird because if we set a password, it is unique for us and should not be known by some other entities. Otherwise, privacy of the password protected system is compromised. But note that people usually make this mistake. In this manner, employees in SD-A has the highest ISA level among the all five of sample domains, which is 76,2% and "satisfactory" as well as SD-B. The other three of sample domains do not share their passwords with someone for any reasons at "average" ISA levels. To remind the Chi-Square values from earlier chapters (Table 1), the intensed tendency that repondents showed in this question is on marking the option, "I do not share with anyone". It can be concluded that the results of this question obviously significant at rate.

3.1.7 Analysis of IS terms and social engineering

Crosstab (Q7*Q38)			Q38. Who is responsible for IS?			Total responses
			Information owner	Information user	Information manager	
Q7. Which sector-department do you work in?	IT sector and IT department	% within which sector-department do you work in?	61,0 % 25	39,0 % 16	70,7 % 29	41
	IT sector and non-IT department	% within which sector-department do you work in?	81,8 % 45	60 % 33	70,9 % 39	55
	Non-IT sector and IT department	% within which sector-department do you work in?	81,4 % 35	34,9 % 15	51,2 % 22	43
	Non-IT sector and non-IT department	% within which sector-department do you work in?	62,9 % 122	48,4 % 94	69,1% 134	194

Table 62 Crosstabulation of Q38 and Q7

In Q38, respondents are asked to know which personnel is exactly responsible for IS within an enterprise, or in the public. If we review the distribution of the rates of the answers, we may claim that SD-A and SD-D think that information managers who are responsible for regulating the flow of information rapidly, accurately and securely among the company, are the only persons for IS.

Crosstab (Q6*Q38)		Q38. Who is responsible for IS?			Total responses
		Information owner	Information user	Information manager	
Q6. Do you work?	Students / graduates (who answered as “No” in Q6)	72,8 % 59	51,8 % 42	69,1 % 56	81

Table 63 Crosstabulation of Q38 and Q6

On the other hand, SD-B, SD-C and SD-E focus on the information owner who are initiators of creating and storing the information in an organization. The option “information owner” is the least chosen answer by the respondents. When we ruminate on IS principals, everyone should have its own part to play for highly protected security around that IS programs assigned. IS is composed of several different countermeasures that everyone has to take, however, everyone is responsible for it.

Regarding the respondents who checked all of three correct options in Q38, the sample domains which reside in “unsatisfactory” ISA level are SD-A 24,3 % (10/41), SD-D 28,8% (56/194) and SD-E 39,5% (32/81) respectively. Employees in SD-C reside in “very unsatisfactory” ISA level with (8/43) 18,6 %. SD-B has the most pleasing level among the others which is at “average” with 49,0 % (27/55). (For simplicity, the dividens like 10, 27, 56, 32 and 8 were not shown. They were derived by filtering the question for each unique option for each sample domain to obtain how many people chose only that option).

Crosstab (Q7*Q39)			**Q39. “A chain is as strong as its weakest link.” What does this motto mean to you?**				Total
			It could cause security vulnerability if an IT personnel walk out	**An IS awareness level in a place is as much as a person who has least IS knowledge in place**	IS is provided only if you have over-experienced technical team	A institution can be exposed to vulnerability if an untrusted employee is recruited	
Q7. Which sector-department do you work in?	IT sector and IT department	% within which sector-department do you work in?	12,2 %	**58,5 %**	19,5%	9,8%	100.0%
	IT sector and non-IT department	% within which sector-department do you work in?	10,9%	**61,8%**	10,9%	16,4%	100.0%
	Non-IT sector and IT department	% within which sector-department do you work in?	9,3 %	**41,9 %**	37,2%	11,6%	100.0%
	Non-IT sector and non-IT department	% within which sector-department do you work in?	6,7%	**52,1%**	24,7%	16,5%	100.0%

Table 64 Crosstabulation of Q39 and Q7

Q39 is asked to participants to obtain if a general security statement has a meaning for them. We can gather from the answers that all five of sample domains know the correct meaning of the motto. From the perspective of ISA level, employees in SD-

A, SD-B, SD-D and students/graduates in SD-E have “average” knowledge about the meaning of the weakest link which is human-being in the chain.

Crosstab (Q6*Q39)		**Q39. “A chain is as strong as its weakest link.” What does this motto mean to you?**				Total
		It could cause security vulnerability if an IT personnel walk out	**An IS awareness level in a place is as much as a person who has least IS knowledge in place**	IS is provided only if you have over-experienced technical team	A institution can be exposed to vulnerability if an untrusted employee is recruited	
Q6. Do you work?	Students / graduates (who answered as “No” in Q6)	18,5 %	**55,6 %**	13,6 %	12,3 %	100.0%

Table 65 Crosstabulation of Q39 and Q6

SD-C is at below the average ISA level, which is “unsatisfactory” although they occasionally have high rates among the other options with 41.9 %. Most notably, students have much more knowledge than employees in SD-C that this finding is unacceptable in terms of employees working in IT department. Why employees in SD-C have unsatisfactorily checked the correct option is because they think that IS is realized by only technical staff in place like network engineers, system administrations or cyber security specialists, which is equivalent to 37,2 % at rate.

Crosstab (Q7*Q40)			**Q40. What does “social engineering” mean?**			Total
			It is a security add-on checking if a website is safe	**It is an art of deception that makes use of abilities of conviction and influence to get information that need to be kept secret**	To be exposed to insultation by an identity you have just met on social media	
Q7. Which sector-department do you work in?	IT sector and IT department	% within which sector-department do you work in?	24,4 %	**70,7 %**	4,9 %	100 %
	IT sector and non-IT department	% within which sector-department do you work in?	25,5 %	**72,7 %**	1,8 %	100 %
	Non-IT sector and IT department	% within which sector-department do you work in?	27,9 %	**69,8 %**	2,3 %	100 %
	Non-IT sector and non-IT department	% within which sector-department do you work in?	38,7 %	**57,7 %**	3,6 %	100 %

Table 66 Crosstabulation of Q40 and Q7

Crosstab (Q6*Q40)		**Q40. What does “social engineering” mean?**			Total
		It is a security add-on checking if a website is safe	**It is an art of deception that makes use of abilities of conviction and influence to get information that need to be kept secret**	To be exposed to insultation by an identity you have just met on social media	
Q6. Do you work?	Students / graduates (who answered as “No” in Q6)	46,9 %	**45,7 %**	7,4 %	100 %

Table 67 Crosstabulation of Q40 and Q6

In Q40, the respondents were asked if they know what social engineering means in security terms. As illustrated above, all of five sample domains have average and above knowledge about social engineering. SD-A and SD-B are at “satisfactory” knowledge while the rest of the participants from other domains have “average” knowledge about the subject.

3.2 Results of Technical Questionnaire

In this section, frequency analysis of two main chapters of technical questionnaire will be demonstrated. The first chapter is titled as demographic features while the second one is more related to tehnical-based focusing on measuring IS awareness of employees and the IS level of network systems of public institutions. To recall, these numbers indicate the awareness level of 20 employees who work in 7 different public institutions and also responsible for managing these network systems which are significantly great in size and sophisticated in design. Proper analysis is conducted with regard to frequency tables in entire chapter.

3.2.1 Analysis of demographic variables

As illustrated in Table 68, respondents in technical survey is generally composed of male participants working in IT department of public institutions. They are mostly at 25-44 and 35-44 age interval. 80 % of them have got undergraduate degree at least. Half of them have 1-3 years experience and other half have 3 years and above working experience. To sum up, we can conclude that our domain have university degree at least and is experienced.

Variables	Subvariables	Frequency	Percent
Q1. Your gender?	Male Female	20 0	100,0 0
Q2. Your age?	< 18 18- 24 25- 34 35- 44 45- 54 > 55	0 0 6 14 0 0	0 0 30,0 70,0 0 0
Q3. What is your (expected) graduate degree?	Upper Secondary School Undergraduate Postgraduate Doctorate	1 16 3 0	5,0 80,0 15,0 0
Q4. Job title?	IS division manager System specialist Analyst System admin Network admin Technician Technical Support Engineer Division supervisor IS Specialist	1 4 1 2 4 1 1 1 5	5,0 20,0 5,0 10,0 20,0 5,0 5,0 5,0 25,0
Q5. Your working experience?	0-1 year 1-3 years 3-5 years 10 years and above	5 5 3 7	25,0 25,0 15,0 35,0

Table 68 Frequency analysis of demographic variables in technical survey

They have number of different job titles such as IS divison manager/supervisor, system and/or network admin, analyst, technical support engineer, technician, support engineer and specialist. The most interesting point is that no one has security title at all but there is nothing to worry with this because employees who were asked for taking the survey were all responsible for security of the systems within the institutions.

3.2.2 Analysis of security standards, procedures and training

This chapter covers 9 questions between Q6 and Q14 to evaluate security standards, procedures and IS training and supporting material use in the institutions. Beginning from this chapter, technical questions are evaluated to measure ISA within the institutions.

Variables	Subvariables	Frequency	Percent
Q6.Which security technologies do you use in your organization? (You can select more than one option)	**Antivirus software**	**19**	**95,0**
	Firewall appliance	**20**	**100,0**
	Web Application Firewall	11	55,0
	Database Firewall	**0**	**0**
	Antispyware software	**17**	**85,0**
	Virtual Private Network	**18**	**90,0**
	Vulnerability/Patch Management	9	45,0
	Data encryption on storage units	9	45,0
	Web / URL filtering	**18**	**90,0**
	Application Firewall	6	30,0
	Log management software	16	**80,0**
	End point security / NAC (Network Admission Control)	9	45,0
	Data loss prevention / content monitoring	**0**	**0**
	Server-based ACLs (Access Control Lists)	**18**	**90,0**
	Information Forensic Tools	**5**	**25,0**
	Public Key Infrastructure (PKI)	**3**	**15,0**
	Smart cards and keys	8	40,0
	Wireless security	**18,0**	**90,0**
	Virtualization specific tools	**19**	**95,0**
	Static accounts user name and passwords	10	50,0
	Biometric	9	45,0
	Information Security Management System (BGYS)	**8**	**40,0**

Table 69 Frequency analysis of Q6

From the illustration above, employees who responsed the survey explain that antivirus/antispyware software, URL filtering, log management, server-based ACLs, firewall appliance and its feature set like VPN, wireless security and virtualization tools have been heavily used in data center which serve 1000 and more end-users.

The most dramatic finding with this question is that none of the public institutions have security technologies, which should be strictly used, like DLP/CM and database firewall. In this respect, we can’t say that data protection in these institutions are provided. These institutions have nothing to do with accidental or deliberate data leaks. One have right to send an intellectual property of an institution to outside via wire or store into flashdisk because the institution doesn’t have a control policy over employees and documents in use. Regarding to database firewall absence, we can’t say that database servers are accurately well-protected by threats even if the institution has a firewall positioned at the edge of the network. It is not incorrect to say that data in database servers are at stake and may be exposed to unauthorized activities by escalation of privilege levels or SQL injection attacks for data theft and leaks. On the other hand, for the low rate of PKI, we can assert that digital certification have not widely well-adopted within public institutions. Additionally, shown that Information Security Management System as well is not used in all of the public institutions.

Q7.Do you follow a standard for network and information security in your organization? If any, select appropriate one(s)? (You can select more than one option)	**a. TS ISO/IEC 27001**	**20**	**100,0**
	b. HIPAA (Health Insurance Portability and Accountability Act)	0	0
	c. PCI DSS (Payment Card Industry Data Security Standard)	0	0
	d. GLBA (Gramm-Leach-Bliley Act)	0	0
	e. COBIT (Control Objectives for Information Technology)	0	0
	f. Another information security standard (optional............)	0	0
	g. None	0	0
	h. I do not have any idea	0	0
Q8. Do you follow any procedure in case of being exposed to cyber-attack?	a. Yes	18	90,0
	b. No	2	10,0
	c. We use another technology/method (optional……)	0	0
Q9. Which information security policies do you put into practice in your organization?	a. Network policies	13	65,0
	b. User policies	9	45,0
	c. Laptop policies	6	30,0
	d. Intrusion Detection/Prevention policies	8	40,0
	e. Patch/Updating policies	8	40,0
	f. Another policy (optional ....)	5	25,0
	g. None of them	0	0
	h. I do not have any idea	1	5,0

Table 70 Frequency analysis of Q7, Q8 and Q9

We can gather from the results of Q7 that all of the public institutions in operations comply with the Turkish Standard ISO/IEC 27001, which is widely known standard.

In general terms, we can think that institutions apply requirements of this standard to keep data assets secured. On the other hand, this fact contradicts to what results we have found in Q6 that there is a vulnerability for database servers and other sensitive data assets as none of the institutions do not use DLP/CM and database firewall technologies. In security standard terms, organizations who comply with a standard should precisely apply the requirements of the standard.

In Q8, we can claim that most of the institutions have a response procedure in case of cyber-attack. In Q9, "network policies" are far more taken care of in comparison with "user policies". The core of the security, "IPS/IDS policies", are appeared to be less important issues to consider as well as "patch/updating policies". Because very few of them chose "another policy" but they did not name it in a way. We can conclude that it is poorly applied within the institution.

Q10. Are your employees being trained about information security awareness?	a. Yes b. Sometimes c. No d. Another (optional…...…………………………)	10 7 2 0	50,0 35,0 10,0 0
Q11. How often do you train your employees about information security?	a. Once a year b. Once a week c. Few times a year d. Once a month	13 0 5 1	65,0 0 25,0 5,0
Q12. Do you follow any resources, materials for oncoming technologic news and developments?	a. I follow some resources at home b. I subscribe to news bulletins and get e-mail regularly c. I benefit from the organization web portal d. I sometimes follow magazines e. Organization training is enough for me f. I do not follow any resource g. Another (optional……………………………….)	4 **12** 3 7 **10** 0 7	20,0 **60,0** 15,0 35,0 **50,0** 0 35,0
Q13.Have you ever experienced any security incident in your organization network? (e.g. threat, attack, malicious software) If any, how many times did you face?	a. 1- 5 times b. 6-10 times c. More than 10 d. Never experienced	9 0 9 2	45,0 0 45,0 10,0
Q14. How long does it take to close the security breaches?	a. Between 0- 3 months b. Between 3-6 months c. Between 6-9 months d. Between 9-12 months	20 0 0 0	100,0 0 0 0

Table 71 Frequency analysis of Q10, Q11, Q12 and Q13

Q10 touches on primary objective of this study. Employees in these public institutions which have complex network systems and great in-scale do not lean on ISA training well. We would hope that they would attend 100% in this question. Proportionally to Q10, they inadequately give training courses for employees about IS issues in Q11.

Q12 concentrates on which IT materials the employees follow on/off the job site. They generally stay informed by IT news bulletins and institution training. Employees who follow resources at home and use other materials are too few. Employees in almost half of the institutions explain that their institutions were exposed to security incidents 1-5 times in past years while the rest faced with such incidents 5-10 times that it indicates such security incidents are usual. Additionally, they state that the incidents could be removed in 0-3 months.

3.2.3 Analysis of firewall, IPS, management, penetration and traffic control

This chapter covers 10 questions between Q15 and Q24 to evaluate various different security points as the header implies.

Variables	Subvariables	Frequency	Percent
Q15. Do you use SSL encryption?	Yes No We use another technology/method (optional.......) I do not have any idea	20 0 0 0	100,0 0 0 0
Q16. Do you use Virtual Private Network (VPN) on your network?	Yes No We use another technology/method (optional……) I do not have any idea	20 0 0 0	100,0 0 0 0
Q17. Do you perform daily logging on your wired network?	Yes No We use another technology/method (optional…..) I do not have any idea	20 0 0 0	100,0 0 0 0
Q18. Do you use xflow protocols on your netwok? (e.g. Netflow, netstream, sflow)	Yes No We use another technology/method (optional……) I do not have any idea	19 0 1 0	95,0 0 5,0 0
Q19. Do you use authentication protocol in your network structure? (You can select more than one option)	TACACS/TACACS+ We do not use RADIUS Smart Card Biometric We use another authentication protocol I do not have any idea	2 0 17 3 4 0 1	10,0 0 85,0 15,0 20,0 0 5,0

Table 72 Frequency analysis of Q15, Q16, Q17, Q18 and Q19

All of the institutions do properly use SSL encryption while their traffic flows out of the inside network to access a website which has SSL encrypted sessions between the employee and webserver. All of the institutions use VPN to communicate over public network- internet with their counterparts in regional branch offices located in geographically separate places. Additionally, employees outside the institution can access to institution intranet to work when they are outside over VPN.

Along with the 5651 act of law, institutions do log daily mandatorily in their networks. In high traffic networks, xflow protocols can enable admins to gather information about traffic flow by sorting particular categories like “application” or “ip address”. These institutions have high bandwidth requirements that can not be thought without the use of xflow monitoring protocols. Most of them have xflow protocols in use.

In Q19, there seems to be high use in RADIUS rather than proprietary solutions like TACACS/TACACS+ authentication server. In security terms, it shows that employees working in public institutions can only access to network services if they are only authenticated first and then authorized to do so. If some of employees in different department are not authorized to access to wireless network or e-mail services in a way, they are only capable of using what they are authorized in RADIUS server settings. Unauthorized access attempts are denied by RADIUS server, otherwise. On the other hand, there are other authentication options like biometric and smartcard but they are not widely used according to answers that participants gave.

Public institutions have been outsourcing to perform some penetration tests for their network systems in order to see how the system are resistant to attacks or if there is any vulnerability or breach. However, they make perform penetration tests for web environment and conduct necessary filtering for web software from the observation of the response rates in Q20.

Q20. Do you make penetration test for web environment?	Yes No We use another technology/method (optional……) I do not have any idea	16 4 0 0	80,0 20,0 0 0
Q21. Do you make necessary filtering for web software?	Yes No We use another technology/method (optional……) I do not have any idea	13 6 0 1	65,0 30,0 0 5
Q22. Do you apply CoPP (Control Plane Policy)/CPU on your network appliances?	Yes No We use another technology/method (optional……) I do not have any idea	10 9 1 0	50,0 45,0 5,0 0
Q23. Is your network infrastructure wired or wireless?	Wired Wired and wireless	0 20 0	0 100,0 0
Q24. Do you have IPS or IDS appliance on your wired network?	We do not use any of them We have IPS appliance but IDS We have IDS appliance but IPS We use both appliances I do not have any idea	0 3 1 16 0	0 15,0 5,0 80,0 0

Table 73 Frequency analysis of Q20, Q21, Q22, Q23 and Q24

As half of the employees stated in Q22, network devices like routers or switches can be down by exposing to basic high traffic load (e.g UDP flooding) which makes CPU load 100% and freezed/crashed. If it happens, routers/switches can not maintain some of its functions properly and drop those functions by causing a chaos in the network. Regarding Q23, all of the institutions have wired and wireless infrastructure in use. As mentioned earlier, Q24 is the most crucial question that IPS/IDS devices are the heart of the security in the network if we want to talk about the security of a network perimeter especially in such great public institutions. Fortunately, many of the institutions have IPS/IDS appliance in use in wired network but if they do not have skilled employees who write/edit signatures against attacks and threats, implementing an appliance alone won’t be securing your network.

3.2.4 Analysis of wireless network security

Similar to Q24 in previous chapter, Q25 asks if institutions have wireless IPS/IDS sensors in place.

Variables	Subvariables	Frequency	Percent
Q25. Do you have wireless IPS or IDS appliance on your wireless network?	We do not use any of them We have IPS appliance but IDS We have IDS appliance but IPS We use both appliances I do not have any idea	4 0 0 16 0	20,0 0 0 80,0 0
Q26. Are your wired and wireless IPS appliances integrated each other?	Yes No	13 7	65,0 35,0
Q27. Do you use guest portal on your wireless network?	Yes No We use another technology/ method(optional..) I do not have any idea	17 3 0 0	85,0 15,0 0 0
Q28. Do you perform daily logging on your wireless network?	Yes No We use another technology/method (optional.) I do not have any idea	20 0 0 0	100,0 0 0 0
Q29. Do you use WEP on your wireless network security?	Yes No We use another technology/method (optional………………………………………...) I do not have any idea	0 20 0 0	0 100,0 0 0

Table 74 Frequency analysis of Q25, Q26, Q27, Q28 and Q29

In Q25, most of respondents express that they have wireless IPS/IDS appliances. One reason to account for why they have to get wired and wireless IPS/IDS devices integrated is that the signature databases in both topologies should be synchronized each other to be awared of same threats and attacks and to protect against threats coming over either network. From this point of view, shown from the responses in Q26 that some of the institutions do not have both IPS/IDS devices integrated each other although they get both wired and wireless sensors. In Q27, expressed that guest portal is provided to meet guest users at the first place. If credentials are known by guests (e.g identity number and temporary password) they join the wireless network to access internet. Guest portal is a kind of ordinary webpage asking for credentials to have guests involved in guest VLAN isolating from production network within the wireless perimeter. In Q28, all of the institutions do keep logs of events occurred in daily basis as well as in wired networks in Q17. Q29 is a reversed question that using WEP in wireless network means that the network is insecure because of using crackable algorithm. Fortunately, all of the institutions do not use deprecated WEP algorithm superceded by WPA in their wireless network.

3.2.5 Analysis of OSI application layer security

Variables	Subvariables	Frequency	Percent
Q30. Do you use voice applications?	Yes No We use another technology/method (optional……) I do not have any idea	15 5 0 0	75,0 25,0 0 0
Q31. Are they encrypted?	Yes No We use another technology/method (optional……) I do not have any idea	5 15 0 0	15,0 75,0 0 0

Table 75 Frequency analysis of Q30 and Q31

Many of the respondents express that they use voice applications such as voice conferencing and IP phoning on their desk phone but the voice data generated are not encrypted in transit.

3.2.6 Analysis of OSI transport layer security

Variables	Subvariables	Frequency	Percent
Q32. Do you find port-based filtering enough?	Yes No We use another technology/method (optional…) I do not have any idea	6 14 0 0	30,0 70,0 0 0

Table 76 Frequency analysis of Q32

Unfortunately, most of the institutions do not apply TCP/IP port filtering in computers and network devices as indicated in Q32. We can state that their intranet can be exposed to internal attacks or TCP/IP based attacks originated by malicious workers.

3.2.7 Analysis of OSI network layer security

This chapter covers only two important questions to evaluate OSI Layer 3 security in the institutions.

Variables	Subvariables	Frequency	Percent
Q33. Which security feature is configured on your Layer 3 Switches or routers?	uRPF (Unicast Reverse Path Forwarding)	0	0
	ICMP redirection	6	30,0
	ACL (Access Control List)	14	70,0
	Fragmentation attack prevention	2	10,0
	Teardrop prevention	0	0
	We do not use these	0	0
	Another technology (optional …….….)	0	0
	I do not have any idea	3	15,0
Q34. Is authentication configured on your routers?	Yes (MD5)	17	85,0
	Yes (Cleartext)	0	0
	No	0	0
	We do not use router (optional……….)	0	0
	I do not have any idea	3	15,0

Table 77 Frequency analysis of Q32

In router interfaces, unicast RPF help limit the spoofed IP addresses on a network by discarding the packets whose IP address is not valid. Also, IT staff who are responsible for configuration of security features do not apply teardrop attack prevention, which cause victim machines crashed or freezed by sending oversized and overlapping IP fragments. It can be concluded that they are mostly awared of restricting certain subnets by ACLs to access somewhere inside and/or outside the private network. Too few of them response that they configure security feature to prevent ICMP redirection attacks and that they have little knowledge about fragmentation attack prevention. Beside these responses, there are also respondents who do not have any idea about these security cautions. In Q34, indicated that routing packets authenticate between routers by MD5 cryptographic hash function while three of them do not have any idea about the topic.

3.2.8 Analysis of OSI data link layer security

In this chapter, all of the questions (Q35-Q47) focus on the security measures that need to be taken on Layer 2 devices, switches in the institutions. In Q35, we may conclude that unused ports are disabled to prevent physical access by another rogue switch to direct traffic over itself by malicious users who can access data center.

Variables	Subvariables	Frequency	Percent
Q35. Are unused ports disabled?	Yes No We use another technology/method (optional…) I do not have any idea	20 0 0 0	100,0 0 0 0
Q36. Is port security enabled on your network?	Yes No We use another technology/method (optional…) I do not have any idea	20 0 0 0	100,0 0 0 0
Q37. Do you use only one VLAN on your network?	Yes No We use another technology/method (optional…...) I do not have any idea	0 20 0 0	0 100,0 0 0
Q38. Do you use Private VLAN (PVLAN) on your network?	Yes No We use another technology/method (optional…) I do not have any idea	20 0 0 0	100,0 0 0 0
Q39. Do you use 802.1x protocol on your network?	Only in wired network Only in wireless network Both of them None of them. We use another protocol(optional……………….) I do not have any idea	0 5 13 1 0 1	0 25,0 65,0 5,0 0 5,0
Q40. Do you use protected port?	Yes No We use another technology/method (optional…...) I do not have any idea	9 11 0 0	45,0 55,0 0 0

Table 78 Frequency analysis of Q35-40

In Q36, port security is enabled on all of the institution switches to allow only specific senders to send traffic those ports by restricting learning number of MAC addresses on the port. Q37 is a reversed question again that sing only one VLAN is a terrible thing to do because using only one VLAN means that all of the end-users, which make 1000 and more in an institution, participate only one broadcast domain. Luckily, all of the institutions have more than one VLAN by dividing the broadcast domains to more manageable and secured parts. Proportional to Q37, institutions use PVLAN which further divides same broadcast domains by providing isolation between ports, that is, more granular control over only one VLAN. This finding also confirms the previous results obtained in Q37. In Q39, most of the respondents state that they use 802.1x authentication protocol as mostly in wired networks. In Q40, protected port disables employees in the institution communicating with each other while they can access to internet via router. We can not conclude that all of the institutions definitely have protected port feature in use.

Q41. Is DHCP Snooping enabled on your network?	Yes No We use another technology/method (optional……) I do not have any idea	20 0 0 0	100,0 0 0 0
Q42. Is ARP Inspection enabled on your network?	Yes No We use another technology/method (optional……) I do not have any idea	20 0 0 0	100,0 0 0 0
Q43. Is IP Source Guard enabled on your network?	Yes No We use another technology/method (optional……) I do not have any idea	10 10 0 0	50,0 50,0 0 0
Q44. Is Root Guard enabled on your network?	Yes No We use another technology/method (optional……) I do not have any idea	7 12 1 0	35,0 60,0 5,0 0
Q45. Is Loop Guard enabled on your network?	Yes No We use another technology/method (optional……) I do not have any idea	20 0 0 0	100,0 0 0 0
Q46. Do you use Storm Control feature on your network?	Yes No We use another technology/method (optional……) I do not have any idea	9 10 1 0	45,0 50,0 5,0 0
Q47. Is MAC Security configured on your network?	Yes No We use another technology/method (optional…....) I do not have any idea	13 7 0 0	65,0 35,0 0 0

Table 79 Frequency analysis of Q41-47

In Q41, DHCP Snooping feature is enabled on switches for all of the institutions that if a rogue DHCP server is set up on the network by a malicious entity, and he/she redirects traffic over itself, by sending its default gateway address to the clients, to sniff the packets. The institution switches with DHCP Snooping feature enabled on ports do not reply to those spoofed default gateway addresses of malicious user. In Q42, ARP Inspection is enabled on switches for all of the institutions that packets are first validated and then forwarded to destination according to trusted IP-to-MAC binding database. With the help of this feature, institutions can prevent ARP cache poisoning attacks in Layer 2 networks that flood rogue ARP responses. In Q43, IP Source Guard feature is not enabled in all of the institutions that half of the security personnel mention that they do not use it. Hence, switches can be exposed to IP spoofing attacks because they do not filter IP addresses on untrusted Layer 2 ports depending on DHCP snooping binding table, so that, one of the hosts can spoof and get IP address of another host. In Q44, we can't see that all of the institutions make use of STP Root Guard feature to prevent their switches from the bad results of setting a false root bridge accidentally. Setting a false bridge can make switches converge incorrectly, even in longer time or misdirect the traffic to unintended way. In Q45, loop guard feature provides extra loop-free topology in some circumstances on highly switched network environments. In this regard, it seems that all of the institutions benefit from this feature in case the bandwidth in use is consumed by packets traversing from one switch to another endlessly without ever reaching destination. In Q46, storm control feature on switched environments drops the traffic that exceeds certain preconfigured threshold value. This is not used by all of the institutions in regard to responses the employees gave. However, shown from the responses that some of the institutions can be exposed to denial of service attacks due to misconfiguration in switches which cause loops or due to unnecessary services sending abnormally excessive messages. Q47 concerns with MACsec feature available at Layer 2 security. Even if most of the respondents state that they have MACsec feature in use, some of others do not use it in a way. For some of others, they do not secure communication between end points so that the data in transit is not confidential and integrity of data is controversial. The data in transit can be monitored and altered by malicious users who have access physically to port in a way.

3.2.9 Analysis of OSI physical layer security

In this chapter, OSI physical layer (Layer 1) will be evaluated with the questions between Q48 and Q57.

Variables	Subvariables	Frequency	Percent
Q48. Do you perform user id authentication in all of the gates of your organization?	Yes No We use another technology/method (optional……) I do not have any idea	11 9 0 0	55,0 45,0 0 0
Q49. Do you have any user authentication mechanism at the entrance of system rooms?	Yes No We use another technology/method (optional……) I do not have any idea	20 0 0 0	100,0 0 0 0

Q50. Do you use shredder to destroy document assets of your organization?	Yes No We use another technology/method (optional…...) I do not have any idea	20 0 0 0	100,0 0 0 0
Q51. Do you have fire sensors in system rooms?	Yes No We use another technology/method (optional…...) I do not have any idea	20 0 0 0	100,0 0 0 0
Q52. Do you have cooling sensors in system rooms?	Yes No We use another technology/method (optional……) I do not have any idea	20 0 0 0	100,0 0 0 0
Q53. Do you have power redundancy in system rooms?	Yes No We use another technology/method (optional…....) I do not have any idea	20 0 0 0	100,0 0 0 0
Q54. Do you have cameras in system rooms?	Yes No We use another technology/method (optional……) I do not have any idea	20 0 0 0	100,0 0 0 0

Table 80 Frequency analysis of Q48-54

In Q48 and Q49, illustrated that not all of the institutions do use authentication mechanism in all of the gates within the organization but at first entrance of the system. All of the institutions use shredder to exterminate sensitive documents. In Q51 and Q52, fire and cooling sensors are present in system rooms for all of the institutions to get informed beforehand in case of excessive temperature fluctuations. Power redundancy is the core of business continuity that all of the institutions have ready-to-use backup power utilities in system rooms. In Q54, cameras are present to monitor and record movement in the system rooms for all of the institutions.

Q55. Are the cabinets locked in system rooms?	Yes No We use another technology/method (optional……) I do not have any idea	15 5 0 0	75,0 25,0 0 0
Q56. Do you label the cables plugged in to network devices?	Yes No We use another technology/method (optional…....) I do not have any idea	18 2 0 0	90,0 10,0 0 0
Q57. Do you have disaster recovery center?	Yes No We use another technology/method (optional……) I do not have any idea	9 10 0 1	45,0 50 0 5,0

Table 81 Frequency analysis of Q55-57

In Q55, cabinets covering all networking equipments and appliances in trays are locked in many institutions. Labelling is also important issue to consider on cables plugging into network devices. Not knowing which cable goes to which device can cause devastating results in great and sophisticated network environments if labelling does not exist. In Q57, we can conclude that almost half of the employees response that they do not have disaster recovery center in case of any natural disaster which disrupts normal operation of devices. When we consider that those couldn't operate and serve the citizens, unprecedented set of problems can arise and harm the nation and country image.

3.2.10 Analysis of end-point security

This chapter covers 3 questions between Q58 and Q59 to evaluate end-point security in the institutions.

Variables	Subvariables	Frequency	Percent
Q58. Do you use a technique that prevents passwords from holding in RAM?	Yes No We use another technology/method (optional……) I do not have any idea	19 1 0 0	95,0 5,0 0 0
Q59. Do you use BIOS password in end point stations?	Yes No We use another technology/method (optional……) I do not have any idea	10 9 1 0	50,0 45,0 5,0 0
Q60. Do you get WHOIS service?	Yes No We use another technology/method (optional……) I do not have any idea	11 8 1 0	55,0 40,0 5,0 0

Table 82 Frequency analysis of Q58-60

As observed in Q58, most of the employees state that they use a technique that prevents passwords keeping in RAM. On the other, it is not convenient to say similar words in Q59. In Q60, once again we can not claim that every institution participated in this survey benefit from WHOIS service which allows query particular registered users of internet resource like IP address class, domain name and many others.

CHAPTER 4

CONCLUSION AND FUTURE WORKS

In this chapter, results of the analysis and discussions that we made in previous chapter are summed up. Strong and weak sides of the public and IT security personnel in public institutions are underlined briefly in both surveys. We also observe that some of the weak sides in technical survey correspond to vulnerabilities found in the event of National Cyber Security Simulation 2011 [29]. Eventually, some requirements and suggestions to develop and increase certain level of ISA at nationwide are discussed.

4.1 Conclusion

During this thesis study, in each chapter of general survey, current posture of the internet users coming from different sector and department, and of the students/graduates were examined. Some evaluations in terms of IS knowledge and behaviours they exhibit in daily life were made when they meet some security incidents. With the application of technical survey, the responses of IT security staff who are responsible for securing network perimeter in public institutions were evaluated that maintain complex and greater data centers. All of them was observed in accordance with the questions defined in main problem and sub-problem statements chapters. Now we will brief the results in which respondents remain weak in order to see overall outlook.

4.1.1 General survey

In order to sum up the results found in the general survey, we can conclude that employees and students who belong to different domains remain weak or strong in knowledge about some of the security topics. We will accurately explain the weak and strong sides of them in this part. Firstly, what we have obtained for each question in the survey will be explained briefly.

Despite the fact that they think that they can face with IS incidents satisfactorily. To recall Q17, shown that all of the respondents do not know sufficiently about Cyber Security Branch Offices affiliated under police departments in the cities where they live when their personal rights are violated on social media/website. Even if they are much more awared of other public authorities like "prosecution offices" and "administration of relative websites" to report security incidents which violate their personal rights, those branch offices are not well-recognized yet for them. Also, students have the lowest rates at reporting to all three authorities when compared to other 4 different groups. Shown that most of the internet users have difficulty in reporting authorities satisfactorily. Lacking in reporting security incidents to correct authorities also corresponds to the similar results found by Öğütçü G. (2010) [8]. Observed from Q18 that they also unwillingly report unwanted content on the internet. In here, they are also much awared of Internet Information Report Center affiliated under the Presidency of Telecommunication (TİB) to report. Only internet users who reside in SD-B are averagely awared of this authority.

In "e-mail security" chapter, employees who do not work in neither IT sector nor IT department can be potential victims for SPAM mails as well as students. Inspite of the fact that most of them know what SPAM means, SD-D and SD-E remain "average" ISA level that they highly chose "I do not have an idea" in Q22. By choosing this option, one can say that participants mean that they may ignore the e-mail or just delete. Is that correct way of behavior? Unfortunately, no. The correct path is to create a new post to ask your friends not to send such SPAM mails trying to get you involved in SPAM chain. In similar manner, in Q23, same sample domains chose "I do not have an idea". The correct behavior is not to open up a file with unknown extension and to create a new post and to send it to original e-mail address of your friend to check if he/she is the person who he/she claims. Because 37.7% of them do not have any idea when they got an e-mail saying that a little girl is lost for a while and they are asked to forward the e-mail to as many people as they can. When we think about the number of participants in this domain, it makes significant amount persons who think forwarding e-mail.

In “safely use of internet and computer” chapter, SD-B, SD-D and SD-E lack knowledge about keeping MAC address of laptops, marking a sign on, installing an alarm and a GPS software to trace remotely in case their laptops are stolen. Note that one of the most important things to do when purchase a laptop is to keep its physical address and serial number. In password protected screen saver use, we can express that only SD-C, SD-D and SD-E remain unsatisfactory awareness level. Same three groups internet users do not use password protected screen saver in both business and home environments. In safe website concerns, the most devastating results are employees in SD-D and students in SD-E have difficulty in differentiating which website is safe or not so that these two groups are not adequately awared of small golden lockpad next to URL line. SD-D has also unsatisfactory level of knowledge about the names of websites starting with https which are SSL encryption enabled. Inadequate knowledge about SSL is also stated by Öğütçü M. in her study (2010) [8]. In ADSL security, important set of features like preventing SSID, activating firewall, checking modem firmware updates and filtering MAC addresses are not widely used by internet users but they should be awared of the presence of such important security features of ADSL modems.

In “threats and preventive measures” chapter, they do not have accurate knowledge about threats coming with P2P file sharing software despite the fact that all of the groups of internet users most commonly use these types of software. They do not think that they will violate copyright of software, music and video files or be exposed to some threats by making files visible to public for the sake of file sharing. SD-B, SD-C and SD-E reside in unsatisfactory levels. In updating software, we can conlude that the employees in SD-D show less care for updating software once the updates are available. They are slightly below average ISA level. In antivirus software use, SD-B, SD-D and SD-E are in favor of purchasing free antivirus solutions by ignoring the wide range of security features that license paid antivirus software include.

In “password management and security” chapter, the habit of changing passwords regularly does not seem to be important by most of groups of internet users except the employees in SD-A. The group of internet users (SD-B, SD-C and SD-D) who remain below the average ISA level usually think that changing is only necessary if they have to give passwords with friends. This finding also overlaps with the results found by Öğütçü M. (2010) and the survey conducted in Ministry of National Education (2012) [8, 14]. Students usually change their passwords if they suspect that it is stolen. Regarding to setting a strong password, we can say that employees in SD-B, SD-D and students do not take care of creating passwords with 16-bit long even if the system allows to do so.

In “IS terms and social engineering” chapter, all of sample domains except SD-B do not know exactly the entities who are responsible of IS concerns. In security terms, there is a widely known statement: “A chain is as strong as its weakest link.” Employees in SD-C think much more different than the others. They think that IS is provided only if you have over-experienced technical team. This is incorrect that many can look at IS issues in that way. When the meaning of “social engineering” is asked to students in SD-E reckon that the “social engineering” is much more like security add-on installed on web browser which checks if a website is safe or not. Even if roughly half of them choose the correct option, shown that their mind is not clear.

To highlight the strong sides briefly, most of the internet users from different backgrounds do not shop on the internet at internet cafes. Most of them do have average and above knowledge about filtering tools that prevent kids from facing with harmful content on the internet. They do not share uniquely identifying personal data on social media like identification number or telephone number. They reckon that they will face with security incidents in the future although they haven’t faced much more. This finding shows that they have certain awareness level about security incidents. Only internet users who reside in SD-B and SD-C averagely know the authorities to report to both “prosecution offices” and “relative websites admins”. SD-D only averagely reports to “prosecution offices”. They know what SPAM means. All of the types of different groups of internet users do not care e-mails coming from banks which ask them to update their personal records. Nevertheless, Adıgüzel stated (2009) that banks should send security warnings and correct way of behaviours, while interacting with ATM or online banking, to make customers stay informed [6]. To continue, they do not trust e-mails which have weird domain name and attachment or SPAM mails except SD-D and SD-E. In case of computer theft, SD-A, SD-B, SD-C and SD-D are good at backing up and encrypting sensitive data and setting passwords for user accounts for taking cautions. SD-E is only good at last two measures. Only SD-A and SD-B exhibit correct way of behaviour in using password protected screen saver by activating it in both business and home computers. Most of the internet users can differentiate which website is safe to surf except SD-D. In ADSL security features, all of the internet users are awared of setting wireless connection password. SD-A, SD-B and SD-C also have average and above knowledge about setting password for web interface, setting wireless password and encrypting the connection between modem and client by WPA/WPA2 algorithm. This finding related to setting wireless password is contradicts what Öğütçü M. (2010) found [8]. Most of the internet users update their software installed in their computers on time without delaying except SD-D. Antivirus use among all of the groups is high. SD-A and SD-C benefit from the important additional features of license paid antivirus software. Security scanning and backing up data are often performed at average and above levels. Great amount of internet users think that firewall and antivirus software should be installed together in a computer as Öğütçü M. also stated in her study (2010) [8]. All of the groups at least averagely set their passwords by using combination of upper, lower letters, numbers and special characters but only SD-A change passwords regularly. All of the groups mostly change when they suspect if the password is stolen by someone. All five groups of internet users do not share their password with someone. Only SD-B think that information manager, owner and user are responsible for IS concerns in a place. On the other hand, only SD-C reckon that an ISA level in a place is as much as a person who has least IS knowledge in place. Most of the internet users except students obviously know what social engineering means. When we take a look at the analysis results of IT sector and IT department employees (SD-A), they appear to have at least average awareness level in many security topics that this finding also supports similar findings as I. Mart expressed in her work (2012) [15]. She states that employees who come from engineering background are most likely to have high awareness levels because they extensively use information technologies in the work [15].

In general survey, 40 questions are asked, which cover basic security topics that we can meet in daily life, to different groups of participants randomly on the internet. Current situation for all of the respondents in different groups of internet users seems to require ISA training especially for their weak sides. By thinking that way, an IS suggestions document was prepared and put at the end of online general survey to make respondents improve in which topics they lack mostly (Appendix C).

4.1.2 Technical survey

In order to put forward an entire posture from the results of technical survey, the strong and weak sides of IT security personnel and the institutions will be summarized. In tehnical survey, 60 questions are asked, which cover several OSI Layer security topics, to IT security employees working in 7 public institutions in Turkey. Observed that some of the vital security features in networking equipments are not in effect. Which threats and attacks can arise due to ignoring those features will be emphasized while explaining weak sides. Then, strong sides will be highlighted as well.

To touch on weak sides in each chapter,

In “security standards, procedures and training” chapter, the most devastating result is that institutions do not have DLP/CM and database firewall. As mentioned earlier, DLP/CM monitors and ensures the safety of sensitive data by preventing employees from taking them out while database firewall protects database servers from malicious activities such as leveraging of privileges of database admins/users or SQL injection attacks. ISA trainings- which is also vital objective of this thesis study are not given properly within the institutions as respondents note in the survey. ISMS is inadequately used in the institutions. Inadequate use of ISMS and giving ISA trainings are the findings which correspond to what found in National Cyber Security Simulation 2011 [29].

In “firewall, IPS, management, penetration and traffic control” chapter, observed that the institutions use SSL encryption, VPN tunnels, RADIUS servers and xflow monitoring protocols while making daily logging in wired and wireless networks, penetration tests at the same time. Filtering web software is not being completely held in institutions that this inadequacy overlaps with the breaches found in web applications of the institutions which participated in National Cyber Security Simulation 2011 [29]. Most importantly, they do not care of control plane policy which protects CPU of network devices from high traffic load by preventing them crashed or freezed.

In “wireless security” chapter, institutions have IPS/IDS devices on wired and wireless networks but the great amount of respondents state that they are not integrated to each other which causes signature databases are not synchronized. In other words, IPS device in the wireless network can not identify the threats coming ingress the port which wired IPS can identify or vice versa. This can be due to employees which have inadequate technical skills. Technical inadequacy of the employees were also reported in National Cyber Security Simulation 2011 event [29]. On the other hand, guests who visit the institutions are asked to log in with credentials to join wireless network by guest portal and also the wireless connection is WPA protected, stronger than preceded version WEP.

In “application layer security” chapter, they heavily use voice applications but voice data is not encrypted in transit. In “transport layer security”, they do not use port-based filtering. In “network layer security”, they inevitably use ACLs and prevent ICMP redirection messages but most notably they are not awared of teardrop attack prevention and unicast RPF. Why these technologies are so lifesaving was mentioned earlier in the analysis of technical survey. Not making certain configurations to prevent teardrop attacks can expose vulnerability to DoS attacks. This finding also gives hint about the vulnerability against DoS attacks in institutions. This result truly confirms one of the results found in National Cyber Security Simulation 2011 that 16 out of 20 institutions were exposed to DoS attack simulated in the event [29]. To continue evaluation, packets of routers firstly authenticate each other with password protection hashed by MD5 algorithm.

In “data link layer security”, unused ports are disabled. 802.1x authentication in use. port security, DHCP snooping and ARP inspection features are enabled while some of the very crucial security features like protected port, IP source guard, root guard, storm control and MACsec are partially used. Not to take storm control in effect can also cause vulnerability against DoS attacks as well as in teardrop attack prevention. Once again, the finding confirms one of the results in the cyber security event carried out in 2011 that some of the institutions can be exposed to DoS attacks [27].

In “physical layer security”, there is no authentication control mechanism at all of the gates of institution but first entrance. In system rooms, power redundancy, fire and cooling sensors, cameras, and labeled cables are present. They also have the shredder to destroy secret and sensitive documents. But note that disaster recovery center is the most valuable thing to have on earth that they do not have disaster recovery centers to get network operations into use and recover rapidly. Non-existence of these centers physically in a well-protected place can result in further monetary loss than investing a datacenter because intellectual property that these institutions keep are valuable.

To highlight the strong sides, all of the respondents state that they have TS ISO/IEC 27001 security standard and a response prodecure against cyber attacks in use within the institution. Most of employees follow news bulletins and organization training to stay aligned with technologic advancements. Firewall appliances, antivirus and antispyware software, web/URL filtering tools, access control lists and virtualization tools are the security technologies used in most of the institutions. Log management protocols like xflow is used. WPA/WPA2 wireless encryption algorithm is used in wireless network. VPN tunnels, SSL encryption, RADIUS servers for authenticating clients and IPS/IDS devices are being used widely. In Layer 2 security features, ARP Inspection, DHCP Snooping and Loop Guard are enabled on switches. Additionally, port security is enabled and unused ports and services are disabled on switches. Packets are authenticated on routers with a password hashed by MD5. Most of the institution divide the broadcast domains into smaller manageable VLANs, that is, they use more than VLAN. 802.1x security protocol are in effect for authentication of clients with the RADIUS server- authenticator. In physical security, they use the technology preventing passwords from holding in RAM. System rooms are being monitored by cameras. The temperature is being sensing by cooling and fire sensors. Power redundancy is provided. Labelling is well-done to prevent mess with cables. Shredders is ready for destruction of sensitive documents.

4.2 Future Works

During this study, the main intention is to outline the awareness level of internet users and IT security personnel in public institutions as pointed out in main and sub-problems chapters. In this regard, some of the suggestions are put forwarded below in order to further improve this study in the future.

More comprehensive surveys are really required to analyze IS awareness of public by extending the number of participants of general questionnaire in this study. As a matter of fact, there is not any survey available targeting all of the citizens of Turkey in the literature. The results of these kind of questionnaires will outline the exact IS awareness posture of the folks in the country. The results of such comprehensive surveys can be utilized in later action plans by checking the progress made in every year. Even more, such surveys for public should be regarded as one of the citizenship duties to contribute national security of the country. Online surveys can be held in one special day (maybe on February- Safe Internet Day). By doing so, any personal data must not be asked or collected. Therefore, these kind of survey studies can baseline for National Cyber Security Simulation events, which takes place every two year, in order to understand the progress of the public. SOMEs in Turkey can be the responsible single point of authority to host such surveys like in CERT in Australia (2014) [20]. When the negative results in general survey is thought, human side in the IS issues is ignored. Some of the authorities responsible for IS incidents are not well-known by the public. ISA raising activites are not being adequately held on TVs, radios or social media. State and relative public organizations put emphasis on contributing public awareness and knowledge by putting plans into action.

As a government plan, upcoming strategies and action plans should be put on paper immediately. Individually, institution-wide and nation-wide awareness need to be built if as a whole country intend to have a say in cyber security. The studies need to be carried out with media, law enforcement efforts and public relations, not only with technical IS team. The representatives in the congress can take active role in the cities where they were elected to trigger/support such plans.

From the idea of forming a technical survey in this study, Cyber Security Council of Turkey or TUBITAK should be upmost responsible centralized authority for auditing, determining and maintaining the security landscape of network and systems in the public institutions and the awareness level of the citizens of Turkey. A technical commitee can design technical questionnaires like in this study or more comprehensive and technical ones, and can update in parallel with changes in technology and threats, then apply it to IT personnel in public institutions

Contrary to one of the results were found in technical survey is that TS ISO/IEC 27001 is in use among public institutions participated to survey but it was observed in the Conclusion chapter that ISMSs are not even used in many important institutions where security need to be strictly provided. ISO and IEC have been established the International Standard that has been prepared to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an ISMS [30]. Up-to-date surveys can be placed in ISMS modules like in Kocamustafaoğulları M. (2012) study [17]. In ISMS environment, experiences and mitigation methods with last cyber security breaches can also be shared. Furthermore, to achieve technical survey study in an institution, institution-specific mobile applications can also be created to be accessed from anywhere anytime by employees for responsing surveys. There are many types of IS awareness raising applications to test IS knowledge in the application stores.

In order to contribute to public awareness, the website of TUBITAK, www.bilgimikoruyorum.org can be further developed to be more specific and technical in the cartoon scenarios. The recognition of the website should be increased by advertising on media. The billboards, web sites and social media accounts of public institutions can be beneficial to attract employees’ attention to IS topic. Nation-wide spot films can also be attractive. The country does not have any one yet in this respect.

More importantly, with the order and approval of relative administration in the government, a unique, well-known, highly reputable and reliable institution should be responsible for auditing, mitigating and maintaining security breaches arised in network appliances in all public institutions of Turkey if institutions have difficulty in doing so. If it is not applicable, each public institution should evaluate and employ the candidates by regarding their skills. In this regard, the state should establish a structure of level of security clearences for IT security job candidates. Hence, not only technical skills are spotted on the candidates but a detailed background check should be conducted to give a level of security clearance to candidate especially if the candidates will be recruited for maintaining the security of the systems in the institution. Human resources should classify the proficiency and expertise like career certification paths as network technology vendors arranged. Proficiencies can be divided into voice, wireless, security, routing/switching, data analyst and so on. Each employee will be absolutely required to have little knowledge other than his/her expertise but not everyone should be expected to implement all of the tasks in each topic. This is one of the most important points how things should be run in IT security in the state. For the skillset of senior candidates, they should have enough experience to manage network security devices like IPS/IDS, and some types of firewalls to protect the network perimeter. They should absolutely know configuring firewall, IDS/IPS sensors and follow the new threats from particular websites and take measures in the devices accordingly such as writing and editing new signatures in the IPS devices. A tough security profession is the person who should be able to edit signatures and fix the false positives in an IPS devices. Some technical and ISA trainings should be given in institutions to make increase their expertise.

The state should have strategies in both offensive and defensive security fields. It should fund some public organizations to prepare in-depth cybersecurity studies as also stated in CERT Australian report (2014) [16]. The strategies in offensive and defensive security can only be achieved if and only if the state mandates the public institutions invest in high quality human resources by regulations and it paves the way of producing national security software and hardware with help of certain set of incentives promoted by itself. Even more, government can initiate such strategic ventures by becoming a partner with private entities until the production initiates. The amount for government funds can be gathered by reducing the waste of public resources in institutions, thereby a well-established single point of centralized authority or present one should audit the procurement of information technology equipments in public institutions. Besides, some of the investments should be left for education system that teachers should be trained to instruct kids about internet ethics, safe and effective use because the internet use has been spreading and even surrounding pre-school age children. As the result of web security questionnaire conducted by TUBITAK indicated, high school/university knowledge are inadequate to use types of software securely [9]. In addition, I. Mart (2012) also expressed in her work, by referring to Tekerek (2012), awareness trainings and education are inadequate for students with respect to the topics like information and computer security [15]. In this regard, all levels in education system should be reviewed to figure out if curriculums in public and private schools include security topics. If we, as a nation, are moving forward to information society, note that there are several cases to be achieved along this way. The vital point is to start with raising awareness, determining shortages and close knowledge and skills gap in public and technical side.

REFERENCES

1. **Çifci H.**, **(2013)**, "*Siber Savaş"*, 1st edition, TÜBİTAK Popüler Bilim Kitapları, Ankara. pp. 2.

2. *"Ulusal Siber Güvenlik Stratejisi 2013-2014 Eylem Planı"*, definitions 1.1/ item I, pp. 4.

3. **Canlı M.**, **(2013)**, "*Siber Güvenlik Rapor*", Ankara Siyasal ve Ekonomik Araştırmalar Merkezi (ASEM), pp. 21.

4. **Akyıldız M. A.**, **(2013)**, "*Siber Güvenlik Açısından Sızma Testlerinin Uygulamalar ile Değerlendirilmesi"*, Graduate School Of Natural And Applied Sciences, Süleyman Demirel University, Isparta, pp. 2.

5. **National Institute of Standards and Technology**, **(2003)**, "*Building an Information Technology Security Awareness and Training Program"*. (NIST Special Publication 800-50). Washington DC: U.S. Government Printing Office, pp. 7-9, pp. 11, pp. 24.

6. **Adıgüzel C. G.**, **(2009)**, "*Güvenlik Endişesinin İnternet Bankacılığı Kullanımına Etkisi Ve Vakıfbank Müşterilerine Yönelik Bir Araştırma"*, Institute of Educational Sciences, Gazi University, Ankara, pp. 60, pp.78.

7. **Kruger H.A.**, **Drevin, L.**, **Steyn T.**, **(2010)**, "*The Use of An Information Security Vocabulary Test To Assess Information Security Awareness"*, Proceedings Of The South African Information Security Multi-Conference, pp. 16-21.

8. **Öğütçü G.**, **(2010)**, "*Analysis of Personal Information Security Behavior and Awareness in E-Transformation Process"*. Department of Statistics and Computer Science, Başkent University, Ankara, pp. 30, pp. 35, pp. 36, pp. 37.

9. **TÜBİTAK BİLGEM, "***Web Application Security Awareness Questionnaire"***,** https://www.bilgiguvenligi.gov.tr/raporlar-kategorisi/web-guvenligi-farkindaligi-anket-sonuclari.html, Ankara.

10. **Takemura T.**, **(2011)**, *"Statistical Analysis on Relation between Workers' Information Security Awareness and the Behaviours in Japan"*, Journal of Management Policy and Practice, pp. 27-36.

11. **Veseli I.**, **(2011),** *"Measuring the Effectiveness of Information Security Awareness Program"*, Department of Computer Science and Media Technology, Gjøvik University College, Norway, pp. 1-10, pp. 63-65.

12. **Al-Shehri Y.**, **(2012)**, **"***Information Security Awareness and Culture. British Journal of Arts and Social Science"*, England, pp. 61-69

13. **The Ministry of National Education (Turkey), (2012)**, "*Information Security Awareness Questionnaire Evaluation Report*", http://bigb.meb.gov.tr/meb_iys_dosyalar/2013_01/03030227_anketsonucdegerlendirme.pdf, pp.4, pp.6, pp.9.

14. **Mart İ., (2012),** "*Bilişim Kültüründe Bilgi Güvenliği Farkındalığı*", Department of Computer and Instructional Technology Education, Sütçü İmam University, Kahramanmaraş, pp. 1-6, pp. 66-72.

15. **Deloitte Touche LLP**, **NASCIO**, **(2012)**, *"2012 Deloitte-NASCIO Cybersecurity Study State Governments at Risk: A Call For Collaboration and Compliance"*

16. **Kocamustafaoğulları M., (2012)**, *"A Prototype Assessment For Assessment Of Information Security Awareness And Implementation Level"*, Graduate School Of Natural And Applied Sciences, Natural and Applied Sciences Mathematics And Computer Science, Çankaya University, Ankara, pp. 1-6, pp. 27, pp. 39, pp. 83.

17. **Pricewaterhouse Coopers, (2013),** "*Key Findings From The Global State Of Information Security Survey 2014*", http://www.pwc.com/security, p.488.

18. **Ernst and Young Global Limited**, **(2013),** "*Under Cyber Attack EY's Global Information Security Survey 2013 Report*", *http://www.ey.com/Publication/vwLUAssets/EY_-_2013_Global_Information_Security_Survey/$FILE/EY-GISS-Under-cyber-attack.pdf*, pp. 4-8, pp. 17.

19. **CERT Australia**, **(2013)**, *"Cyber Crime and Security Survey Report 2013"*, *https://www.cert.gov.au/newsroom* , pp. 5-8.

20. **Microsoft Inc.**, **(2010),** "*Microsoft Security Intelligence Report: Global Botnet Infection Rates (Volume 9)*", pp. 3-5.

21. **Batchelder D.**, **Blackbird J.**, **Felstead D.**, **(2013)**, "*Microsoft Security Intelligence Report: Regional Threat Assessment (Volume 16)*", Redmond, WA, pp. 609- 615.

22. **Bu Z.**, **Dirro T.**, **Greve P.**, **Lin Y.**, **Marcus D.**, **Paget F.**, **Schmugar C.**, **Shah J.**, **Sommer D.**, **Szor P.**, **Wosotowsky A.**, **(2012),** *"McAfee Threats Report: First Quarter 2012"*, Santa Clara, CA, pp. 17.

23. **Kansas Office of Information Technology Services, (2014)**, *"Security Awareness Assessment"*, https://oits2.ks.gov/security/assessment/, Topeka, Kansas.

24. **Stanford University Information Security Office Secure Computing, (2007),** *"Information Security Review Priliminary Questionnaire"*, http://web.stanford.edu/group/security/securecomputing/SU_Security_Assess_v3.html

25. **Houston A.**, **(2014),** "*Anket Hazırlama Klavuzu*", http://istatistikanaliz.com/anket.pdf, pp. 1-50.

26. **Iarossi G.**, **(2006)**, *"The Power of Survey Design: A User's Guide For Managing, Interpreting Results, and Influencing Respondents"*, https://openknowledge.worldbank.org/handle/10986/6975, The World Bank, Washington D.C., United States, pp. 27-80, pp. 147-178.

27. **Purdue University**, **(2014)**, *"Online Writing Lab"*, http://owl.english.purdue.edu/owl/resource/559/06/.

28. **Bilgi Teknolojileri ve İletişim Kurumu**, **TÜBİTAK**, **(2011)**, *"Ulusal Siber Güvenlik Tatbikatı 2011 Sonuç Raporu", pp. 4-9, pp. 21-39.*

29. **European Commission TEMPUS**, *"Report on Existing EU practices for Cyber Security"*, *http://ecesm.net/sites/default/files/Dev%201.1%20-%20v1.0.pdf*, Maribor University, Slovenia, pp. 18.

REFERENCES

FOR IS SUGGESTIONS DOCUMENT

1. **TÜBİTAK BİLGEM**, *"Güçlü Parola Oluşturma",* http://www.bilgimikoruyorum.org.tr/?b222_guclu_parola_olusturma, pp.4, pp.9.

2. **The Ministry of National Education (Turkey), (2012)**, "*Information Security Awareness Questionnaire Evaluation Report",* http://bigb.meb.gov.tr/meb_iys_dosyalar/2013_01/03030227_anketsonucdegerlendirme.pdf, pp.4, pp.6, pp.9.

3. **TÜBİTAK BİLGEM**, *"Zararlı Programlardan Korunma Yolları"*, http://www.bilgimikoruyorum.org.tr/?b314_zararli_programlardan_korunma_icin_neler_yapmaliyim pp5

4. **TÜBİTAK BİLGEM**, *"E-posta Kurum İçerisinde Neler Yapılabilir"*, http://www.bilgimikoruyorum.org.tr/?b433_eposta-kurum-icerisinde-neler-yapilabilir, pp.3–6.

5. **TÜBİTAK BİLGEM**, *"Http Ftp Erişimlerinde Nelere Dikkat Etmeli"*, http://www.bilgimikoruyorum.org.tr/?b423_http-ftp-erisimleirnde-nelere-dikkat-etmeli, pp.4.

6. **TÜBİTAK BİLGEM**, *"İletişim Yolunun Güvenli Olması Nedir?"*, http://www.bilgimikoruyorum.org.tr/?b422_iletisim-yolunun-guvenli-olmasi-nedir, pp.3–7.

7. **TÜBİTAK BİLGEM**, *"Çocuklar İçin Güvenli İnternet"*, http://www.bilgimikoruyorum.org.tr/?b425_cocuklar-icin-guvenli-internet, pp.6.

8. **TÜBİTAK BİLGEM**, *"Bilgi Güvenliğinden Kim Sorumludur"*, http://www.bilgimikoruyorum.org.tr/?b122_bilgi-guvenliginden-kim-sorumludur, pp.3.

9. **TÜBİTAK BİLGEM**, *"Sosyal Mühendislik"*, http://www.bilgimikoruyorum.org.tr/?b320_sosyal_muhendislik, pp.1–7.

10. **TBMM**, **(2007)**, *"İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"*, http://www.tbmm.gov.tr/kanunlar/k5651.html, Kanun No. 5651.

11. **Bilişim STK Platformu**, **(2014)**, http://internethaftasi.org.tr/hafta14/aktif_katilim_cagrisi.php

12. **TÜBİTAK BİLGEM**, *"Güvenlik Olayı Bildirme"*, http://www.bilgimikoruyorum.org.tr/?b124_guvenlik-olayi-bildirme

APPENDICES A

CURRICULUM VITAE

Ahmet Durmus

Network Security Engineer

• +1 (703) 269 73 66 • +90 (532) 410 15 15 • ahmt.durmus@gmail.com • U.S Greencard Holder

PROFESSIONAL SUMMARY

Network Engineer with M.S in Computer Engineering with thesis and B.S. Computer Science degrees, and more than 2 years of experience with internships.

KEY SKILLS

- Experience in manually searching exact matching features of devices in data sheets of the products along with the technical specification documents of tender required
- Experience in using Cisco Dynamic Configuration Tool, Power Calculator and other vendors' tool.
- Experience in configurating network devices on GNS 3 Simulator Tool.
- Experience in IP addressing, R/S, ASA firewall, Cisco IOS, VPN, ASDM on GNS 3 Simulator Tool.
- Experience in network monitoring on Wireshark tool.

PROFESSIONAL EXPERIENCE

IT Consultant, Full Time **December 2012 – October 2013**
Turkish Grand National Assembly, Ankara, Turkey
Turkish Parliament is the 2nd important public institution in the protocol after Presidency.

- Observe and inform the representative about law proposals especially related to IT issues which made him gain hours because he is the member of Industry, Trade, Energy, Natural Resources, Information and Technology Commission in the Turkish congress.
- Managed Twitter account and website of the representative by making news and

- announcements to public

Network Presales Specialist, Full Time **July 2011- May 2012**
Sentim Information Technologies Inc., Bilkent**,** Ankara, Turkey
Leading system integrator IT company with around 500 employees, which is also Cisco, Microsoft and HP partner

- Work with account managers in selling strategies of network devices mostly to public institutions.
- Prepare kitlists with the help of vendors' tools (if any) in timely manner to specify which network devices match with requirements of the public institution in the tender document.
- Prepare estimated price offer sheet for certain kitlists by requesting price offer from distributor companies who sell vendor products like Cisco, HP, Juniper, Enterasys and many others.
- The tender named as "Purchase of Information Technology Equipment" for State Supply Office and Land Forces Command were 2 challenging and important projects studied only by me definitively and which made company earned million dollars and besides, company gained trust for military IT projects from now on.

Software Testing Intern **February 2009- May 2009**
Sentim Information Technologies Inc., Bilkent, Ankara, Turkey

- It was about automation project for one of municipality that variables in the code were matched with project documents to make software developers gain several hours by setting them free of paperwork burden.

Software Testing Intern **July 2008- August 2008**
Meteksan System and Computer Technologies, Ankara, Turkey

- I supported to enterprise resource planning project for Radio and Television Supreme Council of Turkey by helping one of the software developer, who assigned me to change from java code to javascript in a way. It shortened his job by half an hour at least.

EDUCATION

M.S. Computer Engineering **January 2012- September 2014**
Cankaya University, 100. yıl, Ankara, Turkey
(CGPA 3.43)

- **Thesis:** Information security awareness of IT staff and other people were measured statistically in IBM SPSS tool by applying surveys and making some considerable analysis.
- **Application:** Java coded to show the demonstration of how CPU Scheduling algorithms (e.g. FCFS, SJF, FPPS, RRS) work in operating system course.

B.S. Computer Science **September 2005- July 2010**
Bilkent University, Bilkent, Ankara, Turkey
Ranked 98th the best university throughout the world in terms of Engineering and Technology, accredited by the Times Higher Education (THE) in 2014
1 Honor Certificate, CGPA 2.62**Graduation Project:** “Vademecum” medical dictionary like application was developed via Objective-C language for the use of Turkish pharmacists and doctors using i-Pad, i-Phone. Our team was awarded as “Best Senior Project” by an IBM staff.

TRAINING and CERTIFICATES

- **Cisco Certified Network Proffessional Security (CCNP-Security) training,** Cliguru Training and Consultancy, Kizilay, 2014, (24 weeks)
- **Cisco Certified Network Professional (CCNP) training,** Cliguru Training and Consultancy, 2013 (6 weeks)
- **CEH & Security Workshop v2.0 training,** Cliguru Training and Consultancy, Kizilay, 2012, (1-day)
- **Huawei Certified Datacom Associate (HCDA) certificate,** Infopark, Bilkent, 2012
- **Cisco Certified Network Professional-Security (CCNP-S) certificate,** Infopark, Bilkent, 2011
- **Cisco Sales Expert (CSE) certificate,** Infopark, Bilkent, 2011
- **Cisco Certified Network Associate Security (CCNA-S) certificate,** Infopark, Bilkent, 2011
- **Cisco Certified Network Associate (CCNA) certificate,** Infopark, Bilkent, 2010
- **MCTS: Microsoft Windows Mobile Application Development 5.0 certificate,** Infopark Bilkent- Cyberpark, 2009

TECHNICAL SKILLS

Knowledge Areas: well-adapted to CCNA, CCNA Security curriculum, CCNP R/S and Security subjects have been reviewed by CBT Nuggets videos and Cisco books

Programming Languages: Java, C#, HTML, PHP, Objective-C

Database Systems and Tools: MySQL, Sqlite, XCode, Netbeans, Dreamweaver, MS Visual Studio

Other: GNS 3 Network Simulator, Packet Tracer, Cisco Security Device Manager, Cisco Dynamic Configuration Tool, Cisco Feature Navigator, Cisco Power Calculator, Cisco OIP, Wireshark

ACTIVITIES

Playing basketball, making fitness, jogging and reading management and IT security stuff

APPENDICES B

GENERAL SURVEY FORM

Dear survey participants,

The results of this questionnaire are going to be used in master thesis titled “Information Security Awareness in the Public” in Çankaya University- Institute of Natural and Applied Science. The purpose of this survey is to contribute positively to secure use of computer and internet and the awareness of information security.

Achieving the objective is based on your precious contribution. Therefore, reading and answering the questions carefully is all that matters. Please be convenient that it is not asked for identifying information such as name, surname and identification number of participants.

All of the questions can be answered roughly in 10 minutes. You are not allowed to backward to previous questions. If you are interested in, downloadable “Information Security Awareness (Suggestions)” document might attract your attention at the end of the survey.

Thanks for your kind contributions in advance.

Ahmet DURMUŞ

CHAPTER 1 – DEMOGRAPHIC FEATURES	
Q1.Your gender?	Male Female
Q2.Your age?	<18 24 34 44 54 >54
Q3.Which city do you live in?	Select from rolling down list

Q4.What is your (expected) graduate degree?	a. Primary School b. Secondary School c. High School d. Upper Secondary School e. Undergraduate f. Postgraduate g. Doctorate
If you chose a/b/c option in previous question, skip to 6th question. Go ahead otherwise.	
Q5.In which faculty/ institute/ college/ upper secondary school did you study?	Select from rolling down list
Q6.Do you work?	a. Yes b. No
If you chose option 'b' in previous question, skip to 9th question. Go ahead otherwise.	
Q7.Which sector- department do you work in?	a. IT sector- IT department b. IT sector- non-IT department c. Non-IT sector- IT department d. Non-IT sector- non-IT department
Q8.Your working experience?	a.0-1 year b.1-3 years c.3-5 years d.5-10 years e.Above 10 years

CHAPTER 2 – SECURITY INCIDENT AND REPORTING	
Q9.Do you use internet?	a.Yes b.No
If you chose option 'b' in previous question, the survey ENDS. Go ahead otherwise.	
Q10.How much time do you spend on the Internet?	a.Very little b.Little c.Average d.Much e.Very much
Q11.Do you shop on the Internet?	a.Certainly yes b.Yes c.Sometimes d.No e.Certainly no

Q12.Do you know about the filtering tools that prevent children from seeing unwanted contents on the Internet?	a.Nothing b.Very little c.Average d.Much e.Very much
Q13.Do you have a membership for any social media platform like Facebook, Twitter, Instagram and so on?	a.Yes b.No
If you chose option 'b' in previous question, skip to 15th question. Go ahead otherwise.	
Q14.Which personal information that you mostly share in social media?	a.Picture b.Video c.Name, surname d.Birthdate e.Name, surname of family members f.Identification number g.Phone number h.E-mail address i.Researches/studies k.Emotions l.Thoughts m.Hobbies
Q15.Have you ever faced with negative incident about information security?	a.Yes b.No
If you chose option 'a' in previous question, skip to 10th question. Go ahead otherwise.	
Q16.Do you think that you will probably face with such incidents in the future?	a.Yes b.No
Q17.You faced with a content in a social media or a website that violate your personal rights. Where do you report?	a. My family and/or friend b. The nearest police department c. Relative website admin d. Internet Service Provider e. Internet Information Report Center (Telekomünikasyon İletişim Başkanlığı İnternet Bilgi İhbar Merkezi) f. Cyber Security Branch Office g. Prosecution Office h. I do not know where to report i. I do not report
Q18.When you faced with a unwanted content (encourage/help suicide and prostitution, harmful drugs, gambling, nudity, sexual harassment and crimes against Atatürk etc.). Where do you report?	a. My family and/or friend b. The nearest police department c. Relative website admin d. Internet Service Provider e. Internet Information Report Center (Telekomünikasyon İletişim Başkanlığı İnternet Bilgi İhbar Merkezi) f. Cyber Security Branch Office g. Prosecution Office h. I do not know where to report i. I do not report

CHAPTER 3 – E-MAIL SECURITY	
Q19.Do you use e-mail address?	a.Yes b.No
If you chose option ‘b’ in previous question, skip to 24th question. Go ahead otherwise.	
Q20.What is SPAM?	a. SPAM is an antivirus solution b. SPAM is a firewall c. SPAM is an unwanted and mass e-mails d. SPAM is an e-mail attachment
Q21.What do you do when you got an e-mail asking to update your personal info by clicking the link in the e-mail body?	a. I click the link if logo and address of the bank is right b. I do the same if my close friends update their info c. I make a call to bank to get information about the e-mail d. I do not have any idea
Q22.What do you do when you got an e-mail saying that a little girl is lost for a while and ask you to forward the e-mail as many people as you can?	a. I forward to all of my contacts b. I forward to closest contacts c. I create a new post to ask sender not to forward chain e-mail d. I do not have any idea
Q23.What do you do when you got an e-mail from your friend but file extension of the attachment and domain name of the address (the section after ‘@’ sign) is weird?	a. It is safe to open up attach as the sender is friend of mine. b. I reply to e-mail to confirm if it is really sent by my friend c.I create new post to send to my friend’s address in my contact to for confirmation d. I do not have any idea

CHAPTER 4 – SAFELY USE OF INTERNET AND COMPUTER	
Q24.Which countermeasures do you take in case your laptop is stolen?	a.Keep its physical (MAC) address b.Keep its serial number c.Backup my sensitive data d.Encrypt my sensitive data e.Install an alarm software f.Set passwords for my user accounts g.Mark a sign to a unrecognizable place on my laptop h.Install a GPS software to trace remotely
Q25.Do you activate screen saver with password when you took a little break to return in the middle of your studies?	a. I only activate in my business laptop b. I only activate in my personal computer c. I use it in both d. I do not activate as I go back to work in short time e. I do not activate as my data is not that critical
Q26.How do you distinguish if a website is a safe to surf or not?	a. Websites that offer freeware are safe b. Online casinos are safe c. It is safe if a security logo exists d. It is safe if the web browser shows small gold lockpad e. It is safe if its address starts with “https://” instead of “http://” f. It is safe if it appears to be popular g. I am having difficulty in distinguishing

Q27.Which security measures below do you take in your ADSL modem?	a. Shut down my modem when I do not use it b. Set a password for web interface c. Set a wireless connection password d. Encrypt connection between computer and modem via WPA/WPA2 e. Prevent SSID broadcast f. Shut down unused and unnecessary services g. Activate modem firewall h. Filter MAC address(es) i. Check modem firmware updates
CHAPTER 5 - THREATS AND PREVENTIVE MEASURES	
Q28.Have you ever used peer-to-peer file sharing software like Kazaa, LimeWire, uTorrent, eMule and so on?	a. Yes b. No
If you chose option 'b' in previous question, skip to 30th question. Go ahead otherwise.	
Q29.Which ones are the threats originated by peer-to-peer file sharing software?	a. I may violate copyright of music, video or any other software b. The program I downloaded may include malicious software c. I may allow bad guys with bad intentions to see my personal data
Q30.What do you think about updates of your types of software installed in your computer?	a. I install at once if there is available update b. I install few days later after I take care of my other tasks c. I get help from my closest friends d. I do not have any idea
Q31.What type of antivirus software do you use in your computer?	a. I use free antivirus software b. I use cracked antivirus software c. I use license paid antivirus software d. I do not use antivirus software e. I do not have any idea
If you chose option 'd' in previous question, skip to 31st question. Go ahead otherwise.	
Q32.How often do you make security scanning in your computer?	a. Never b. Rare c. Average d. Often e. Very often
Q33.How often do you backup your data in your computer?	a. Never b. Rare c. Average d. Often e. Very often

Q34.Which one of the statements below is true?	a. Only firewall is sufficient in a computer b. Only antivirus software is sufficient in a computer c. Both antivirus software and firewall perform same functionalities d. Both antivirus software and firewall need to be used updated in a computer
CHAPTER 6 - PASSWORD MANAGEMENT AND SECURITY	
Q35.What do you think about changing your passwords?	a. I change my password only if I doubt that somebody stole it b. Changing process is boring c. I change my password regularly d. I change my password only if I have to give it to my friend
Q36.How do you set your password?	a. I use the password preset by the system b. I set short password not to forget c. I set all of my passwords same not to forget d. I set my password including upper, lower letters, numbers and special characters e. I set my passwords with 8 characters at least if the system allows f. I use password generator tool
Q37.With whom do you share your computer's authentication password?	a. I share with my trusted friend b. I share with my trusted relative c. I share with IT division in my corporate d. I don't share with anyone
CHAPTER 7 - IS TERMS AND SOCIAL ENGINEERING	
Q38.Who is responsible for IS?	a. Information owner b. Information user c. Information manager
Q39."A chain is as strong as its weakest link." What does this motto mean to you?	a. It could cause security vulnerability if an IT personnel walk out b. An IS awareness level in a place is as much as a person who has least IS knowledge in place c. IS is provided only if you have skilled technical team d. A corporate can be exposed to vulnerability if an untrusted employee is recruited
Q40.What does "social engineering" mean?	a. It is a security add-on checking if a website is safe b. It is an art of deception that makes use of getting information that need to be kept secret in normal circumstances by using convincing and influencing abilities c. To be exposed to insultation by an entity you have just met on social media

*****We are so glad to take our questionnaire*****

Contact: bilgiguvenligianketi@outlook.com

APPENDICES C

TECHNICAL SURVEY FORM

Dear survey participants,
The questionnaire is going to be used in master thesis, entitled "Information Security Awareness in our society" in Çankaya University Institute of Science. The purpose of this survey is to contribute positively to secure use of computer and internet and the awareness of information security.

Achieving the objective is based on your precious contribution. Therefore, reading and answering the questions carefully is all that matters. Please be convenient that it is not asked for identifying information such as name, surname, id, from participants.

All of the questions can be answered roughly in 10 minutes. You are not allowed to backward to previous questions. If you wish, downloadable "Information Security Awareness (Suggestions)" document might attract your attention at the end of the survey.

Thanks for your kind contributions in advance…
Ahmet DURMUŞ

CHAPTER 1 – DEMOGRAPHIC FEATURES	
Q1.Your gender?	a. Male b. Female
Q2.Your age?	a. < 18 b. 18- 24 c. 25- 34 d. 35- 44 e. 45- 54 f. > 55
Q3.What is your (expected) graduate degree?	a. Primary School b. Secondary School c. High School d. Upper Secondary School e. Undergraduate f. Postgraduate g. Doctorate
Q4.Your job title?	(……………………………………………………)

Q5.Your work experience?	a. 0-1 year b. 1-3 years c. 3-5 years d. 5-10 years e. Above 10 years
CHAPTER 2– SECURITY STANDARDS, PROCEDURES AND TRAINING	
Q6.Which security technologies do you use in your organization? (You can select more than one option)	a. Antivirus software b. Firewall appliance c. Web Application Firewall d. Database Firewall e. Data Leakage Prevention f. Antispyware software g. Virtual Private Network h. Vulnerability/Patch Management i. Data encryption on storage units k. Web / URL filtering l. Application Firewall m. Log management software n. End point security / NAC (Network Admission Control) o. Data loss prevention / content monitoring p. Server-based ACLs (Access Control Lists) q. Information Forensic Tools r. Public Key Infrastructure (PKI) s. Smart cards and keys t. Wireless security u. Virtualization specific tools w. Static accounts user name and passwords v. Biometric x. Information Security Management System (BGYS) y. Other (optional…………………………………………………)
Q7.Do you follow a standard for network and information security in your organization? If any, select appropriate one(s)? (You can select more than one option)	a. TS ISO/IEC 27001 b. HIPAA (Health Insurance Portability and Accountability Act) c. PCI DSS (Payment Card Industry Data Security Standard) d. GLBA (Gramm-Leach-Bliley Act) e. COBIT (Control Objectives for Information Technology) f. Another information security standard (optional......................................) g. None h. I do not have any idea
Q8. Do you have any procedure in case your systems are being exposed to cyber-attack?	a. Yes b. No c. We use another technology/method (optional………………….) d. I do not have any idea
Q9. Which information security policies do you put into practice in your organization?	a. Network policies b. User policies c. Laptop policies d. Intrusion Detection/Prevention policies e. Patch/Updating policies f. Another policy (optional ....) g. None of them h. I do not have any idea

Q10. Are your employees being trained about information security awareness?	a. Yes b. Sometimes c. No d. Another (optional……………………………….)
If you chose option ‘c’ in previous question, please skip to 12nd question. Go ahead otherwise	
Q11. How often do you train your employees about information security?	a. Once a year b. Once a week c. Few times a year d. Once a month
Q12. Do you follow any resources, materials for oncoming technologic news and developments?	a. I follow some resources at home b. I subscribe to news bulletins and get e-mail regularly c. I benefit from the organization web portal d. I sometimes follow magazines e. Organization training is enough for me f. I do not follow any resource g. Another (optional…………………………………….)
Q13.Have you ever experienced any security incident in your organization network? (e.g. threat, attack, malicious software) If any, how many times did you face?	a. 1- 5 times b. 6-10 times c. More than 10 d. Never experienced
Q14. How long does it take to close the security breaches?	a. Between 0- 3 months b. Between 3-6 months c. Between 6-9 months d. Between 9-12 months
CHAPTER 3- FIREWALL, IPS, MANAGEMENT, PENETRATION AND TRAFFIC CONTROL	
Q15. Do you use SSL encryption?	a. Yes b. No c. We use another technology/method (optional………………….) d. I do not have any idea
Q16. Do you use Virtual Private Network (VPN) on your network?	a. Yes b. No c. We use another technology/method (optional………………….) d. I do not have any idea
Q17. Do you perform daily logging on your wired network?	a. Yes b. No c. We use another technology/method (optional………………….) d. I do not have any idea

Q18. Do you use xflow protocols on your netwok? (e.g. Netflow, netstream, sflow)	a. Yes b. No c. We use another technology/method (optional………………….) d. I do not have any idea
Q19.Do you use authentication protocol in your network structure? (You can select more than one option)	a. TACACS/TACACS+ b. We do not use c. RADIUS d. Smart Card e. Biometric f. We use another authentication protocol (optional...) g. I do not have any idea
Q20. Do you make penetration test for web environment?	a. Yes b. No c. We use another technology/method (optional………………….) d. I do not have any idea
Q21. Do you make necessary filtering for web software?	a. Yes b. No c. We use another technology/method (optional………………….) d. I do not have any idea
Q22. Do you apply CoPP (Control Plane Policy)/CPU on your network appliances?	a. Yes b. No c. We use another technology/method (optional………………….) d. I do not have any idea
Q23. Is your network infrastructure wired or both wired and wireless?	a. Only wired b. Both wired and wireless
Q24. Do you have IPS or IDS appliance on your wired network?	a. We do not use any of them b. We have IPS appliance but IDS c. We have IDS appliance but IPS d. We use both appliances e. I do not have any idea
CHAPTER 4- WIRELESS NETWORK SECURITY	
Q25. Do you have wireless IPS or IDS appliance on your wireless network?	a. We do not use any of them b. We have IPS appliance but IDS c. We have IDS appliance but IPS d. We use both appliances e. I do not have any idea
If you did not chose options 'b' or 'd' in both 25th and 26th questions, please skip to 27th question	
Q26. Are your wired and wireless IPS appliances integrated each other?	a. Yes b. No

Q27. Do you use guest portal on your wireless network?	a. Yes b. No c. We use another technology/method (optional………………….) d. I do not have any idea
Q28. Do you perform daily logging on your wireless network?	a. Yes b. No c. We use another technology/method (optional………………….) d. I do not have any idea
Q29. Do you use WEP on your wireless network security?	a. Yes b. No c. We use another technology/method (optional………………….) d. I do not have any idea
CHAPTER 5- OSI APPLICATION LAYER SECURITY (LAYER 7)	
Q30. Do you use voice applications?	a. Yes b. No c. We use another technology/method (optional…………………) d. I do not have any idea
If you chose option 'b' in previous question, please skip to 32nd question	
Q31. Are they encrypted?	a. Yes b. No c. We use another technology/method (optional…………………) d. I do not have any idea
CHAPTER 6- OSI TRANSPORT LAYER SECURITY (LAYER 4)	
Q32. Do you find port-based filtering enough?	a. Yes b. No c. We use another technology/method (optional…………………) d. I do not have any idea
CHAPTER 7- OSI NETWORK LAYER SECURITY (LAYER 3)	
Q33. Which security feature is configured on your Layer 3 Switches or routers?	a. uRPF (Unicast Reverse Path Forwarding) b. ICMP redirection c. ACL (Access Control List) d. Fragmentation attack prevention e. Teardrop prevention f. We do not use these g. Another technology (optional ………….…………)
Q34. Is authentication configured on your routers?	a. Yes (MD5) b. Yes (Cleartext) c. No d. We do not use router (optional………………………………………..)

CHAPTER 8- OSI DATA LINK LAYER SECURITY (LAYER 2)	
Q35. Are unused ports disabled?	a. Yes b. No c. We use another technology/method (optional………………….) d. I do not have any idea
Q36. Is port security enabled on your network?	a. Yes b. No c. We use another technology/method (optional………………….) d. I do not have any idea
Q37. Do you use only one VLAN on your network?	a. Yes b. No c. We use another technology/method (optional………………….) d. I do not have any idea
Q38. Do you use Private VLAN (PVLAN) on your network?	a. Yes b. No c. We use another technology/method (optional………………….) d. I do not have any idea
Q39. Do you use 802.1x protocol on your network?	a Only in wired network b. Only in wireless network c. In both of them d. None of them e. We use another protocol (optional ....) f. I do not have any idea
Q40. Do you use protected port?	a. Yes b. No c. We use another technology/method (optional………………….) d. I do not have any idea
Q41. Is DHCP Snooping enabled on your network?	a. Yes b. No c. We use another technology/method (optional………………….) d. I do not have any idea
Q42. Is ARP Inspection enabled on your network?	a. Yes b. No c. We use another technology/method (optional………………….) d. I do not have any idea
Q43. Is IP Source Guard enabled on your network?	a. Yes b. No c. We use another technology/method (optional………………….) d. I do not have any idea

Q44. Is Root Guard enabled on your network?	a. Yes b. No c. We use another technology/method (optional………………….) d. I do not have any idea
Q45. Is Loop Guard enabled on your network?	a. Yes b. No c. We use another technology/method (optional………………….) d. I do not have any idea
Q46. Do you use Storm Control feature on your network?	a. Yes b. No c. We use another technology/method (optional………………….) d. I do not have any idea
CHAPTER 9- OSI PHYSICAL LAYER SECURITY (LAYER 1)	
Q47. Is MAC Security configured on your network?	a. Yes b. No c. We use another technology/method (optional………………….) d. I do not have any idea
Q48. Do you perform user id authentication in all of the gates of your organization?	a. Yes b. No c. We use another technology/method (optional………………...) d. I do not have any idea
Q49. Do you have any user authentication mechanism at the entrance of system rooms?	a. Yes b. No c. We use another technology/method (optional………………….) d. I do not have any idea
Q50. Do you use shredder to destroy your institution documents?	a. Yes b. No c. We use another technology/method (optional………………….) d. I do not have any idea
Q51. Do you have fire sensors in system rooms?	a. Yes b. No c. We use another technology/method (optional………………….) d. I do not have any idea
Q52. Do you have cooling sensors in system rooms?	a. Yes b. No c. We use another technology/method (optional……………) d. I do not have any idea

Q53. Do you have power redundancy in system rooms?	a. Yes b. No c. We use another technology/method (optional……………) d. I do not have any idea
Q54. Do you have cameras in system rooms?	a. Yes b. No c. We use another technology/method (optional……………) d. I do not have any idea
Q55. Are the cabinets locked in system rooms?	a. Yes b. No c. We use another technology/method (optional……………) d. I do not have any idea
Q56. Do you label the cables plugged in to network devices?	a. Yes b. No c. We use another technology/method (optional……………) d. I do not have any idea
Q57. Do you have disaster recovery center?	a. Yes b. No c. We use another technology/method (optional……………) d. I do not have any idea
CHAPTER 10- END POINT SECURITY	
Q58. Do you use a technique that prevents passwords from holding in RAM?	a. Yes b. No c. We use another technology/method (optional………………….) d. I do not have any idea
Q59. Do you use BIOS password in end point stations?	a. Yes b. No c. We use another technology/method (optional………………….) d. I do not have any idea
Q60. Do you get WHOIS service?	a. Yes b. No c. We use another technology/method (optional………………….) d. I do not have any idea

APPENDICES D

IS SUGGESTIONS DOCUMENT

“Security can not be rushed”
“Different measures need to be taken for different threats”
“Security will never be 100% achieved”
“So there are duties to achieve by everyone”
“Safe and reliable cyber world come true with the measures we all will take”

1) Our operations need to pay attention in internet cafes

We should prefer using our own personal computers to internet cafes in which shared network is used (e.g airports, cafes).
In addition to this, we should confirm the validity of security certificate and the presence of SSL encryption seen at the bottom of the web browser (gold small padlock) to ensure if the shopping website is safe.

- Additionally we should check if the URL of website starts with “https://” instead of “http://”.

- While we are typing personal information (more commonly credit card data) on a website, it is important security indication to provide customers with a pop-up keyboard as attackers are capable of obtaining our key strokes when the website is compromised.

- We should check our credit card receipt if we shopped on the internet.

- We should use virtual credit card if possible and check its limit.

- We should not tell internet banking passwords to anybody including bank clerks

Important note: You can check your bank website for further details about internet banking security issues and announcements under internet banking tab.

2) **Please note that we need more care about unauthorized sharing of information!**

Cyber world is not that different from real world. Most of people do not consider this fact while surfing on the internet.

As there are crimes and penalties in real world, there are also crimes and sanctions in cyber space. Sharing information of someone without consent could result in commiting a crime. Information owner has right to denunciate you.

3) **We should be careful about sharing our personal data!**
When you lost your identification card/credit card what would you do? Of course you renew because malicious persons can get your personal information and make you involve in situations you really do not desire. It becomes more of an issue when it comes to which ones of personal data we use in social media sites. We should hold back to share information that might cause security breach. For example; since identification card data, name and surname of family members, phone number are identifying key words, not to share would be more convenient. On top of that, we should note that it is possible to combine of some of personal data might reach other data or whole identity. Think about 2 or 3 security questions that your bank clerk asked in order to identify your credentials. Recently other identifying personal data is being used, such as voice recognition, fingerprint or retina, to add extra security layer in some places.

4) **How would you form your passwords?**

While setting a password;

- Create new passwords rather than using startup prior passwords [1].

- Set your passwords with 8 characters if possible [1].

- Include special characters "?, @, !, #, %, +, -, *, %" in addition to using upper and lower letters in your passwords [1].

- Not to use rookie passwords that will be easily guessed such as birthdate, name, surname etc [1].

- Not to use dictionary words or common words that every user could generate

- We can form strong passwords composed of memorizable capital letters of daily sentence/lyrics/adage etc [1].
    - Two heads are better than one. 2Ha,bt1[1].
    - My graduate date 6th November, 2010. Mgd6n, 2010 [1].
    - As in the example, number, special character, letter are used in combination [1].
    - Prevent using passwords although they look like strong. For example; 123qwe, 123qweasd, abc123, 123qqqQ vb [1].

- Creating and changing password policies are developed in some organizations. Every employee is responsible for obeying to what policies require [2].

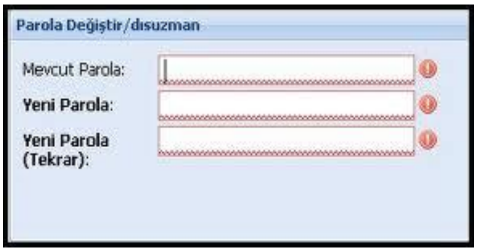
5) We need to gain the habit of changing password!

- Our passwords are like our house keys. They are not for giving to the closest friends, our managers at work, IT specialists etc. On top of that, we give big responsibility to those who we gave passwords in a violation of information security issue.

- We should not forget that we are responsible for the operations that the individuals carry out with our passwords we gave.

- We should not give our passwords to anybody in verbal or written [1].

- Security experts advise you to change your passwords once every six months or shorter and not to use same passwords at more than one place because having an account compromised means that others are also compromised [1].


Parola Değiştir/dısuzman

Mevcut Parola:

Yeni Parola:

Yeni Parola (Tekrar):

- Changing password in regular intervals is not as annoying as having compromised by malicious persons. The best practice is to gain this habit.

6) Please note that banks do not require us to update our personal data via e-mail.

- Banks absolutely do not ask for personal data of their customers via e-mail [2].

- It is not that hard to forge bank logo, address and other information by malicious persons. It is very likely to direct you a forged website, which is exactly the same as original, via a link in the e-mail without your suspect.

- If your friends trust in these links and update their data, their data is not at trusted hands from now on. Because every individiual is responsible for own security. Friends giving personal information for forged e-mail and not experiencing any security issue for now does not mean that they will not be compromised next time. You do not know how and when malicious entities benefit from these data.

- The better practice would be to deleting these kind of e-mails, ignoring them or the best one would be to have a call to bank customer services in order not to be exposed to fraud.

Important note! Banking Association of Turkey advise you to use updated and licensed operating system, antivirus software and firewall and to check they are up while you are operating on internet banking services. You can check your bank website for further details about internet banking security issues and announcements under internet banking tab [2].

7) SPAM e-mail is an unsolicited and mass e-mails

SPAM (Stupid Pointless Annoying Messages) are, as its name implies, annoying, pointless and continuously incoming bulk e-mails/messages. The way to get rid of such e-mails is to mark as unnecessary message "spam" by directing to spam box next time when they arrive.

8) We should neither open nor reply to e-mails with suspicious attachments coming from untrusted sources!

These kind of mails is most probably SPAM. The best practice is to delete e-mail, call the e-mail owner (if recipient is your friend) or to create new e-mail by sending a confirmation e-mail to ensure if your friend really sent to you.

9) We should pay attention to e-mails coming from the person we know!

- Most of the time we would install malicious software without consent by opening the attachment of an e-mail which is supposed to come from the persons we know

- As e-mail fraud is widely-faced security issue, we need to know characteristic of it to form defending practice. By doing this, we need to take care domain name of e-mail addresses (the part following ‘@’). The former part of ‘@’ sign is same as your friend’s address while latter part is different.

- We might cause infecting other user’s computer by forwarding this e-mail as well as replying to the e-mail.

- The best practice is to create a new e-mail and to send this e-mail to our friend’s address in our address book or to make a call to ensure if he/she really sent us.

- It might possibly be a forged website directing us to another website designed to steal our personal data. To prevent such situations we have to copy and paste the link on the address line in the browser.

10) **Emotion traders continue their presence in cyber world! We need to pay attention to incoming e-mails about this issue.**

- It is very likely to receive such e-mails. In general questionnaire, there is a question saying that one little girl is lost for months if you could forward e-mail to many persons as possible as you can. If you have time you can ask for police department if this situation is real but common purpose is to involve people in chain e-mailing to get their e-mail addresses.

- We need to know what blind carbon copy (bcc) stands for. While sending an e-mail to many receivers, putting an e-mail address on bcc field to prevent others’ e-mail address seen by other recipients.

- Another similar e-mail fishing method is to claim “Win 1,000,000 million dollar or exclusive holiday chance if you click the link”. Do not count on it. Please remind that reliable companies do not set up their marketing strategies on such chance games [3].

- Having these kind of e-mails counted on by your friends do not mean that it is convenient practice. You should not reply to e-mails that appears to be suspicious [4].

  Please do not download the attachments with unknown file extensions. You can unconsciously install a spyware making a backdoor on your computer [4].

11) **We can easily notice if a website is safe to surf.**

- The websites serving free chat and software, betting, pornography include highly include malicious software in general. You are more likely to see insistent pop-up windows and advertisements in such sites [5].

- It might not indicate that a website which has security logo in its page is safe to be surfed. These security logos especially embedded botttom of the page might be forged by hackers.

- You can check if the security certificate of the website is still valid by hovering small gold padlock sign on status bar of the web browser [6].

- If the address of the websites starts with “https://” instead of “http://” shows that the traffic between your web browser and server of the websites is encrypted against eavesdroppers or wiretappers. If they eavesdrop the traffic, they can only get encrypted data not a cleartext [6].

- You should not be trapped by the popular appearance of a website [6].

- Please remind that filtering software preventing children from facing inappropriate contents on internet which are provided by Internet Service Providers, operating systems and 3rd party solutions [7].

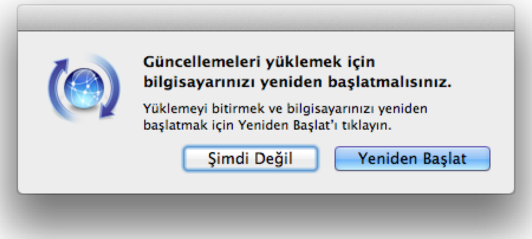
12) **We should not only encrypt our valuable data but also we should back up!**

Backing up is not difficult. You need to give importance and to leave enough time. Think about a second you lost your valuable data which not backed up. How annoying is it? Additionally, when you do not back up your encrypted data you do not have anything to do despite losses. You only prevent malicious users from reading your data. Please note that backing up is another security measure to take. Do not ignore it!

13) **We should not use software whose trial period is outdated!**

Software companies do not announce any updates or supports to those whose trial period is outdated (commonly 30/90 days). Upgrading is already not allowed users who have trial period but only allowed them buy a license to utilize new functionalities. These kind of outdated software could breach the computer security. Because of that we need to use last updated version of software in our PC. If trial period is over, we either find similar software performing same functionalities or buy a licensed version.

14) We should maintain our PCs as we used to do routinely in our cars.



Güncellemeleri yüklemek için bilgisayarınızı yeniden başlatmalısınız.

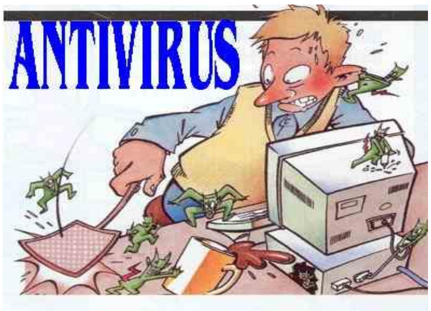
Yüklemeyi bitirmek ve bilgisayarınızı yeniden başlatmak için Yeniden Başlat'ı tıklayın.

- ➢ Everyone is responsible for its own safety. Authorization can be shared but responsibility. It is not good practice to pass security issues on someone else.

- ➢ Operating system, antivirus software and firewall must be licensed, updated and well- operable.

- ➢ It should be downloaded without time loss when new updates are available. Producers of security software can announce new updates because there might be a weakness in the software or new functionalities are up. Because of this reason, installing updates lately mean that you operate your computer with those weaknesses and without new functionalities such as finding a new virus.

15) We have to use antivirus software with firewall together. We should not ignore regular security scanning!



Antivirus software are designed to prevent unconsciously installed malicious codes, software from infecting computers by automatically taking control. But we need to start a manual security scanning in some circumstances. Some of them are when;

- ➢ Software in your PC malfunctions or functions inconsistently,
- ➢ Adding or removing a file without our consent,
- ➢ Computer perceptibly slows down, web browser connects to unknown websites,
- ➢ Firewall or antivirus software is disabled automatically
- ➢ New add-ons are added to web browser,
- ➢ Pop-up and advertisement windows continuously come up,
- ➢ You make web searching and come up with irrelevant results.

16) **Very basic security measures that we do not that much give importance might get us into trouble. Because of that we need to pay attention every security measure!**

Please remind that we can turn to behaviours only by gaining and repeating habits. Security of entrance to computer system increases as much as the data we store increase. When we do not store significantly valuable data in our home computers, we might not use screen saver with password but it is beneficial to make a habit on behalf of every user.

17) **Every individual in society is responsible for information security. Information security composed of measures that everyone has to take.**

- Academic studies indicate that information security is not only technical issue but human factor should be well traced, identified and developed at very first phase. Because of that this issue should be carried on by not only a group of people or individual but by everyone who are employed responsibly. Developing, spreading and sharing this knowledge is highly important.

- In a regular company, information security is not only performed in IT department but each department should be responsibly trained for information security awareness because employees who lack information security awareness in knowledge are potential candidates to unconsciously breach security perimeter of an organization for hackers.

- Studies indicate that security perimeter of organizations become compromised due to lacking knowledge in information security awareness despite of the fact that IT department take all the technical measures that have to be taken. However, this means how human awareness matters in this subject.

- Everyone is responsible for information security in a country. Having high-level and over-experienced technical security engineers are not well enough to form a secure cyber space but everyone should play its part responsibly for secure cyber space.

- Because of this reason, information owners, managers and users are all responsible [8].

- It is only possible to mention about information security in place if all of them are responsible. However, how secure we are is based on how aware we are. It is essential to form the same high degree of awareness at each employee working in each department.

18) **We might increase the possibility of reacquiring stolen laptops with the help of few basic measures that has to be taken beforehand.**

When you bought new laptop or PC, be advised to store its MAC address and serial number. This measure eases your laptop being found when stolen. Additionally, setting password for user accounts, backing up and enrypting valuable data, marking a sign onto your laptop, using GPS and alarming software are other measures to take.

19) **The important things that you need to know about file sharing peer-to-peer software:**

We might open sharing in our operating systems with the help of file sharing software in order to share commonly music and video. By doing this, person who need these files can reach and download with P2P software. So can we. We should really ensure if we have to pay attention to violating copyright of a file, downloading software including malicious code or learning how far we open our files for sharing.

20) **Hackers that do know social engineering methods can get valuable information as easy as walking in the park.**

- Social engineering is an art of cheating on people in basic terms. The typical feature of such attack is based on convincing, affecting and sometimes flirting with victims to obtain valuable information that should not be shared in normal circumstances [9].

- Social engineers sort our friends and personal traits of us verbally to gain trust. It could sometimes happen as complimenting and flirting. When you do not consent or agree with them, they stress that you have to rush or bear consequences. They state you that they are authorized persons and they do not become pleased when you asked a question [9].

To protect yourself,

- Training should be held in organizations. Every employee and guests have to wear identification card on. Informative e-mails, websites and brochures might be beneficial for employees within organization [9].

- Valuable documents of companies should be exterminate with a shredder [9].

- As an individual we might follow the websites pertaining to information security concerns [9].

- We should set voice of tone while we are chatting outside places. Be remind that social engineers might benefit from our words coming out our mind outside by collecting other data from social media sites. It appears to be paranoia but not impossible [9].

- We should not leave personal data on the table written on piece of paper. We should thow valuable documents off via shredder if possible [9].

- We should not tell our name and surname to people we do not know [9].

21) **We might face information security incident anytime anywhere. We have to know personal rights and get things done within the legal framework.**

- Please follow your personal rights and inform and warn people. Be remind that we are not only being a role model with these efforts but we also contribute to form a safe cyber world in this regard at the same time. In our country, 5651 act is regulated about "Regulating Contents and Fighting Against Crimes Committed By These Contents On The Internet"[10]. One aspect of being a information society is to develop a youth, using internet effectively, also who has developed ethical and moral codes, internalised information security and privacy in deep and also to develop a high school graduates, whatever the interests, passion, ability they have, who have deep apprehension about basic terms of information technology such as capabilities, borders and bad usage of it [11].

- As most of people do not know the regulations or in where to seek right, they would be a victim. Even more, they act with *"I can handle it"* mentality. Be reminded that the best way is practice of laws.

There are two ways that we can consult when we face with information security incidents on the internet. One of them is to contact with content owner in "contact us” tab. If you face an issue in social media, use reporting functions or get

- information from “Support/Help Center” before you contact with content owner. The second way is to apply legal authorities to begin a legal process. Thus, when you face any insulting and offending contents violating personal rights, the authority where you can obtain information about the issue is **Cyber Security Branch Offices** in cities.

ihbar
web
Telekomünikasyon İletişim Başkanlığı
İnternet Bilgi İhbar Merkezi

- Internet Information and Report Center, tied to Telecommunication Presidency, named TIB in Turkish, have been accepting reports and complaints from citizens about any inappropriate content such as encouraging/driving suicide, harmful drugs, nudity, sexual abuse, gambling, procuring, crimes against Atatürk etc. (link as follows: http://www.ihbarweb.org.tr/) [12].

- There are guiding suggestions for families in the following web address: http://www.guvenlinet.org

- The things you have to do in Twitter when you are subjected to any violation of right (threat, abuse, offensive words etc.) in the following link: https://support.twitter.com/articles/20170499-ihlaller-nasl-bildirilmelidir

- For complaints in Facebook see https://tr-tr.facebook.com/help/

APPENDICES E

GLOSSARY FOR SURVEYS

TS ISO/IEC 27001 is an international standard that defines and manages comprehensive security procedures and risks by explaining the aim of ISMS within an organization. The standard was developed by one of committee of International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). The abbreviation “TS” means that this standard was translated to Turkish by Turkish Standards Institution.

Health Insurance Portability and Accountability Act (HIPAA) is a standard composed of some executive, physical and technical countermeasures that protect privacy of patients’ health data. The organizations that handle these health data and transfer over, or on the internet must implement the responsibilities of the standard (e.g pharmacies, drug stores, health and accident insurance companies, individual doctor cliniques etc).

Payment Card Industry Data Security Standard (PCI DSS) is an international standard that was developed to protect cardholder databy applying to the entities involved in payment card industry- storing, processing or transmitting cardholder data.

Gramm- Leach- Bliley Act (GLBA) is a standard that aims to protect the privacy of personally identifiable information of customers from disclosure in banks, security and insurace companies and to safeguard these organizations.

Control Objectives for Information Technology (COBIT) is a globally accepted IT governance guidance composed of policies, objectives and controls to help companies benefit from IT assets effectively and increase their market value by allowing managers to improve their alignment to business needs well throughout organization.

Worms are kind of malicious code that replicates them without the participation of user as in which viruses require.

Viruses are malicious software which has unique as their behaviours such that some of them install themselves in an executable file so that when the user starts the executable files, the code is immediately run and some others are programmed to infect some specific files in hard disk so that when the user starts the infected file malicious code is run and your computer is infected. Unlike worms, viruses need some end-user activation to replicate themselves.

Anti-virus software is a computer program that detects, prevent, remove malicious program (e.g virus, worms) which has ability to interfere with the normal functionality of a computer by recording, corrupting, deleting data or spread themselves to other computers throughout the network or even Internet.

Spyware is a kind of computer program that has malicious purposes such that it helps gathering information about people or taking control of user privileges without their knowledge. They sometimes implement their functionalities as a keylogger to monitor users, as an adware to user’s Internet surfing habits to redirect to a website or to cause annoying immediate pop-up Windows, and as a trojan horse to gain remote access by causing a “back door” in victim’s system or to cause immediate damage.

Anti-spyware is a computer program that prevents malicious spyware (e.g trojans, adware) exploiting the computer.

Stupid Pointless Annoying Messages (SPAM) is flood messages which is sent to many users on the internet. It is sometimes wasting to delete SPAM messages in your message box. Users who are sending these kind of messages called spammers and they have got significant amount of e-mail addresses in their base.

Peer-to-peer (P2P) file sharing software enables users swap various files (commonly multimedia) on the peer-to-peer network, e.g. Bittorrent, Kazaa, LimeWire, eMule, uTorrent. The idea is that clients open sharing privileges of files to become downloadable from other peers in P2P network. Files with larger size can be downloaded in pieces from other peers who have the same file in their computer. File sharing is legal unless the content is not copyrighted. Another matter to consider is that some of P2P networks include many types of malicious software infected to shared files with/without awareness of clients.

Firewall is sometimes solely a type of software or a dedicated hardware (appliance) in a changing network environment. It protects inside (private) network from the external threats of the world by some certain allowing/denying (filtering) rules for connections traversing through itself. Firewalls have also the capability of recording and reporting on events. Some type of firewalls has the functionality as IPS/IDS appliances do. Firewall productsare divided into few types regarding the techniques in which they monitor the traffic such as packet filtering, stateless filtering, and deep packet inspection.

Web Application Firewall (WAF) is an appliance that protects your network from some form of sophisticated web-based attacks such as HTML/XML inspection, SQL injection, XSS cross-site scripting, identity/data theft and fraud, cookie tampering and so on. It is especially designed to suit the needs for credit card companies and SaaS providers that would like to increase profitability through web-based applications and that collaborates PCI DSS.

Database firewall is a kind of WAF that protects database from incoming attacks (e.g SQL Injection and Buffer Overflow) aiming to hooksensitive information by monitoring access logs, checking white list composed of approved of SQL statements and suspicious activities.

Intrusion Detection System (IDS) is software or an appliance that is positioned behind the firewall to protect the network from internal and external attacks and threats by copying the traffic to be analyzed. Intrusion Detection Systems appear passive in conrast to IPS devices since the traffic doesn't flow over the IDS. An IDS device detects malicious traffic in different ways such as signature-based, policy-based, and anomaly-based and honey pot detection. IDSs can be classified into Network-based IDS (NIDS), Host-based IDS (HIDS) etc.

Intrusion Prevention System (IPS) is a security applicance that implements same functions with IDS such as monitoring network traffic for malicious activities. The difference is that IPS devices are active in the network that they are able to prevent/block malicious traffic that are detected and also positioned inline of the network in contrast to IDS. IPS devices detect the traffic in the similar manner the IDS devices used to do. IPSs can be classified into NIPS Network-based IPS (NIPS), Wireless IPS (WIPS), and Host-based IPS (HIPS) etc.

Authentication is the process of identity check to approveif users or administrators are who they claim to be. A network environment might have variety of mechanism for authentication such as username-password, token cards, smart card, and biometrics and so on.

Network Admission Control (NAC) ensures that every endpoint users (wired, wireless, remote users) conform with proper network security policies before they can access to network. If an endpoint user cannot comply with policies, its access attempt is denied, restricted or moved to quarantine. NAC devices realise users, their devices and the roles in the network.

IEEE 802.1x protocol is a Layer 2 network protocol defines standards for how Extensible Authentication Protocol (EAP) frames are encapsulated over LAN (EAPOL), generally between three parties; supplicant (e.g PC, laptop), authenticator (e.g switch, wireless access point) and an authentication server (e.g RADIUS or a host running software supporting EAP protocols).

Remote Authentication Dial-In User Service (RADIUS) is a network client/server protocol that provides Authentication, Authorization and Accounting (AAA) protocol to control access the network resources. It is typically used by ISPs and enterprises to manage access to Internet or intranet through modems, DSL, VPN and wireless technologies. It uses UDP protocol and connections are not encrypted unlike TACACS+.

Terminal Access Controller Access-Control System Plus (TACACS+) is publicly documented network access control protocolfor routers, network access servers and other network devices. Unlike RADIUS, it provides TCP transport, independent AAA services and also encrypted connection.

Secure Socket Layer (SSL) is a security protocol that secures communications between web browsers (client) and web servers throughout Internet. SSL uses public key infrastructure to secure communication. The web sites built for e-trading especially benefit from this security protocol to protect customers' credit card information by encryptying traffic between client and server. In respect to this, the common deployment of SSL protocol is in Hypertext Transfer Protocol (HTTP) known as https. It is also used in File Transfer Protocol (FTP) and sending e-mail.

Virtual Private Network (VPN) provides a dedicated commnication tunnel between two or more locations (nodes) over a public infrastructure, typically Internet. VPN tunnel does not provide encrypted traffic alone. To do this there are some various types of VPN technologies such as IPSec VPN, SSL VPN, DMVPN, Site-to-Site VPN and so on.

Public Key Infrastructure (PKI) is widely used network technology- which is a framework for network services such as encryption, authentication and non-repudiation. PKI solves the secrecy problem of public key exchange between two entities in asymmetric encryption design by coming up with trusted third party, commonly called "certificate authority" (CA).

Log management software can store huge amount of logs every single day to provide vital information for network administrators about system downtime, network anomalies, user behaviours, policy violations, internal and external threats, login attempts and so on. There are many log management software of different vendors in the market.

Patch and vulnerability management is a security practice to prevent malicious entities from exploiting IT vulnerabilities within an organization. Vulnerability management identifies, classifies, remediates and mitigates vulnerabilities in software system. Patch management is involved in removing security flaws on time, or gaining additional functionality for IT systems when new releases are available.

Data Loss/Leak Prevention (DLP) is a data security solution to monitor, manage and protect confidential and valuable information -whereever it is stored or used- being lost within the organization. Data loss and data leak is sometimes used interchangeably but it is so obvious that they are different. DLP prevents confidential information of organizations' from being exposed by moving from company resources to another location like cloud, USBs, laptops, mobile devices and even personal e-mail accounts. DLP solutions achieve this by controlling and monitoring the sensitivity of content and user-generated trafficwithin organization like HTTP/HTTPs, IM, FTP, SMTP/TLS, Facebook, Dropbox and even the traffic sent from iPads, iPhones over ActiveSync.

Web/URL filtering allows controlling access specific websites including violance or pornography based on URL listthe network administrators created. It also prevents web-based threats from infecting your production network increasing productivity.

MAC Address filtering is a security measure that authenticates users by looking up their physical addresses (MAC Address) which is unique to each PC and predefined beforehand in modem/switch configuration. However, if this filtering mechanism is enabled on devices, only users whose MAC address is predefined in the filtering list can access to resources. No other users are allowed.

Disabling Service Set Identifier (SSID) broadcast is a security measure in wireless access points which broadcast its wireless network name (SSID) to introduce clients who want to join the wireless network. If this option is disabled, no one can know the presence of the network even if you know user name and password credentials.

Access Control List (ACL) is a security measure that is composed of list of permissions to control which users are allowed to access network resources with that of which rights. It is considered as control point in real life.

Network-based Access Control List is a security mechanism composed of set of rules that is run in routers and other Layer 3 devices to restrict user access by permitting or denying according to Ip addresses, ports and certain packet types.

Server-Based Access Control List is a security mechanism thatdescribes the access rights of users, whose authentication is granted, for a resource (e.g file or directory) in the server. Sales department does not have right to write over a file while engineering department could have read and write rights in an organization.

Penetration test (Pentest) is the process of gaining access to network resources with the permission of authority, without any knowledge of means of access, to find security weaknesses before an attacker could find and exploit it. A pentester should have a hacker mindset with the knowledge of both defense and offense side.

Digital forensic tools are kind of software that is designed to help identify, preserve, recover, analyze and present digital information stored in computers for legal evidence.

Wired Equivalent Privacy (WEP) is an IEEE 802.11 standard security algorithm for wireless communications intended to create wired-equivalent secure communication. It is especially presented as first wireless security option in router/modem configurations but it is deprecated tobe used after Wi-Fi Protected Access (WPA) was ratified.

Captive Guest Portal is a special web page in order to authenticate users before they access to Internet in Wi-Fi hot spots, apartment houses, universities, hotel rooms and so on.

Paper shredder is a device that shred your confidential documents, papers into small and unreadable chads. It is so necessary for government organizations, businesses and private individuals to protect their garbage against dumpster divers.

Media Access Control (MAC) Security, typically known MACsec, is a Layer 1 security feature that encrypts your communication, via symmetric cryptography, starting your MACsec-compatible network interface card (NIC) to another NIC between endpoints on wired LANs.

Fire and cooling sensors help prevent potential fire disasters by letting administrators know the actual value of system rooms to take precautions before high temperature rates could disrupt the efficient working of networking devices in system room.

Network cabinets are fitted with doors, side panels and racks for mounting network devices such as switches, routers, servers and so on. Practical cabinets should typically have places to wind cables plugging towards the devices.

Labelling is something very important in networking to be conducted well not to get into trouble with network topology. Labelling help network administrators know with respect to which cables are connected to which devices in order to outline the topology.

Disaster Recovery Center is a backup system room or data center in which most of vital networking devices and services are backed up in against the emergency situations in which network systems are out of use and business continuity does not operate due to human-induced or natural disaster. Disaster recovery center is so indispensable that it might be deemed to a second heart of organizations.

Social Engineering is the art of tricking people to gather information that must be kept securely in normal circumstances by using convincing and affecting methods on human psychology within the context of information security.

Awareness Training, in the context of information security, is an ISAP for organizations to educate all employees monthly or annually to raise awareness for information security, threats and misuse of computer and internetand so on.

Port-based filtering is the security practice of enabling and disabling TCP/UDP ports in computers or network appliances to protect both internal and external network from security attacks and threats incoming from these specific TCP/UDP traffic.

Protected ports are security feature used when the traffic generated by some of applications in your network are not required to be forwarded to another ports in the same switch.

Port security is a Layer 2 security feature for Layer 2 devices (typically switches) to protect Layer 2 Fast Ethernet/Gigabit Ethernet ports from unknown MAC Addresses. When configured on the switch, ports can proactively respond to some attempts. To examplify, when the switch reaches the maximum number of learned MAC addresses in its table, it doesn’t allow learning new ones through a secured port. If a new frame reaches with unknown MAC address to the port in which certain port security features are enabled, frames either might be dropped, or port is shutdown, or both dropped and a log message is sent. These events are named “port security violation”. One more feature to add to port security, unused ports and services should be shutdown in order to harden a switch, router, firewall or even PC.

Virtual Local Area Network (VLAN) is a logical division of a single Layer 2 network, whose aim is to divide single broadcast domain into more manageable isolated domains. These isolated domains can pass packets to each other via routers or Layer 3 switches. What VLAN really does is that a single domain can be divided into management, sales or engineering VLANs corresponding to departments in an organization. This design provides more granular control over network in terms of security, VLAN-based policies and traffic load induced by broadcast packets. Having a single VLAN for an organization with 1000 employees could dramatically degrade network performance by considerably preventing utmost benefits from high-end network infrastructure.

Private VLAN (PVLAN) provides Layer 2 security measure between Layer 2 ports in PVLAN within a single VLAN. PVLAN isolate ports accessing each other within groups. This enables more restriction inside VLAN covering PVLAN such that any user in a management/sales department might not send trafficto another user in the same department.

IP Source Guard is a port-based Layer 2 security feature to prevent malicious hosts masquerading as a trusted host by spoofing their source IP adresses. To do this, the feature prevents hosts in the same network from having same IP addresses by keeping track of IP Source Binding or DHCP Snooping Binding database.

Root guard is a Layer 2 security feature in switches that is also enhancement to spanning-tree protocol (STP), which prevents Layer 2 forwarding loops by creating single path, that it prevents switches with lowest bridge priority from becoming root switch to affect path design. Attackers might connect a rogue switch which has lowest bridge priority to the ports with disabled-root guard feature of other switches in the network to redirect traffic over itself for capturing.

Loop guard is also known as STP Loop Guard, is an additional check to Layer 2 STP loop prevention mechanism that it makes ports, which are not receiving the BPDU messages anymore, move to STP loop-inconsistent blocking state rather than listening / learning / forwarding state. If it is disabled, non-designated ports which are not receiving BPDU messages turn into forwarding state and create loops.

Dynamic ARP Inspection is a Layer 2 security mechanism that prevents responding malicious and invalid ARP requests in the same VLAN. To illustrate, an attacker might send a gratuitous ARP messages to the user to assign its own MAC Address by poisoning the real default gateway of user while sending similar another GARP message for router. However, it directs traffic over itself and sends to router without recognizing the user for long time. This type of attack is often considered as Man-In-The-Middle attack.

Storm Control is a security feature that protects the switch from processing unusual excessive broadcast, unicast or multicast traffic induced by denial-of-service (DoS) attackers, network misconfiguration or user-based and likewise. Storm control is disabled in switches by default, that is, it must be enabled and apply to ports.

DHCP Monitoring calls for a typical monitoring tool to help watching DHCP Server health and availability in the networks in which the server has critical importance.

ICMP Redirection is one of the packet types of Internet Control Message Protocol (ICMP) that is used to help hosts find out which optimal route and appropriate routers can be accessed in the LAN to pass through. When a unique host wants to send a packet through a router, router checks the packet destination address and look up its routing table. If it finds the match, it routes packet out to its available next-hop address while it sends an ICMP Redirect message for informing the host about the best route at the same time. These ICMP packets might be compromised by attackers to poison host routing tables to misdirect the traffic, however, it should be disabled.

Unicast Reverse Path Forwarding (URPF) is a security feature that enables routers limit malicious traffic to prevent IP address spoofing in unicast traffic and ensure loop-free forwarding of multicast packets on a network by verifying source address of packets being forwarded.

Control Plane Policy (CPP) is a security feature that protects routers' processor (CPU)- referred to as Control Plane (CP) which is one of four logical functional parts of a router, from unnecessary, malicious or heavy load by allowing administrators configure Quality of Service filtering mechanism for more granular control over traffic flow. It is crucial to configure this feature on routers operating in business environments especially intolerant to network outages because CP is responsible for many critical network operations such as routing updates, processing packets, network management and so on.

Teardrop attack is a kind of DoS attack that aims to disrupt operativeness of older version operating systems such as Windows 95/NT and Linux kernel by sending fragmented packets with a bug in one of the fields in the IP header of the packet (fragment offset field). When a server received the packet, it can not reassemble because fragment offsets are different from each other and they overlap. This situation results in denial of service of the server operating system.

Xflow protocols are used by monitoring tools which are intended to monitor IP traffic information. Netflow and sFlow are some examples.

Router authentication is a security measure to prevent routers from exchanging false routing updates by unfriendly parties. Router authentication is enabled by configuring a pair of same key at both two neighbouring routers.

Password protection in Read Access Memory (RAM) comprises some security techniques that prevent from getting user accounts' passwords in personal computers or servers running on certain operating systems. With some penetration techniques, it is possible to acquire user account password in Windows operating systems while session is running in the PC.

Cyber Incidents Response Team, abbreviated as SOME in Turkish, was established in 2013 to protect computer networks of the Turkish state from cyber attacks. According to act, every ministry has right to make an own Cyber Incidents Response Team to protect against hostile attack and is responsible for reporting these attacks to higher authorities beforehand.