**YILDIRIM BEYAZIT UNIVERSITY**

**GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES**


# IMPORTANCE OF INFORMATION SECURITY AWARENESS

**M.Sc. Thesis by**

**Şehnaz Hilal MOĞOL**

**Department of Computer Engineering**

**January, 2016**

**ANKARA**

# IMPORTANCE OF INFORMATION SECURITY AWARENESS

**A Thesis Submitted to the**

**Graduate School of Natural and Applied Sciences of Yıldırım Beyazıt University**

**In Partial Fulfillment of the Requirements for the Master of Science in**

**Computer Engineering, Department of Computer Engineering**

**by**

**Şehnaz Hilal MOĞOL**

**January, 2016**

**ANKARA**

## M.Sc THESIS EXAMINATION RESULT FORM

We have read the thesis entitled **"Importance of Information Security Awareness"** completed by **Şehnaz Hilal MOĞOL** under supervision of **Assoc. Prof. Dr. Fatih KOYUNCU** and we certify that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Assoc. Prof. Dr. Fatih KOYUNCU

Supervisor

Prof. Dr. Fatih V. ÇELEBİ

(Jury Member)

Asst. Prof. Dr.Bülent TUĞRUL

(Jury Member)

Prof. Dr. Fatih V. ÇELEBİ

Director

Graduate School of Natural and Applied Sciences

# ETHICAL DECLERATION

I have prepared this dissertation study in accordance with the Rules of Writing Thesis of Yıldırım Beyazıt University of Science and Technology Institute;

- Data I have presented in the thesis, information and documents that I obtained in the framework of academic and ethical rules,
- All information, documentation, assessment and results that I presented in accordance with scientific ethics and morals,
- I have gave references all the works that I were benefited in this dissertation by appropriate reference,
- I would not make any changes in the data that I were used,
- The work presented in this dissertation I would agree that the original,

I state, in the contrary case I declare that I accept the all rights losses that may arise against me.

# IMPORTANCE OF INFORMATION SECURITY AWARENESS

## ABSTRACT

Far today's Word, information security is one the most important topic for every steps in life and every country. To keep the information organizations and countries spend many resources, forces and moneys. Based on this, to know much more about how to keep the information safety we must know what security is and how we can apply this in our systems.

By using the standards and the good security structure, every company and organization, even regular persons can keep their information in safe. But only security programs and standards are not enough to protect. At the same time awareness education and training are really important. Because if there is a security in the system, but user cannot know about how to use it usefully, we cannot get full performance. For this reason, every certain period's organizations should prepare seminars to aware them.

At this point, Information Security Awareness Programs involve the situations. When a company apply the security program and use the standards then it must prepare security awareness program for every person. With this method everyone learns how to protect the data. With long period awareness programs, people are used to apply the program details and provide continuity to protect the data.

In the thesis, first of all, information security and which standards can be used in information security systems are explained. Then, to aware the people for protecting the data from dangerous, different types of information security awareness steps and applying awareness methods to people are explained. For the awareness methods, there are some examples that companies and other organizations are used in.

In the thesis, we give some examples of companies and awareness programs usage percentages. Using this information we can see that, which companies or organizations can really protect their data from dangerous. By using this result, we can see that, how many companies can use the information awareness programs. How many of them really know about any information about awareness programs and if they can use these

programs, what kind of awareness methods they can use. Having this results, we get some idea for our country. Are we really aware of dangerous, or do we really use the methods and protect the information.

Besides, if the companies or regular persons don't know anything about protecting data, it doesn't mean that they cannot learn anything. From the past to today, everyone has progress for information security. Every year, through the seminars, many companies, organizations and people learn more about protecting information. Preparing more information security awareness programs, many people learn more about security too. And after several years, there are no such big hole in the information security area.

On the other hand, in the thesis it is emphasized that why information security is so important for companies. There are five examples for companies which are lose big moneys because of losing information.

In this thesis, some questions related to information security are answered and got some ideas about what can be done for the future period to protect the information and to understand how the information security awareness is so important to use for everyone.

Finally, "Information Security Awareness Survey" was applied with different group of people with different learning levels and places. We measured knowledge levels with this survey. People have learned new information during the survey. Through this survey, the level of knowledge of people in different groups were compared.

**Keywords** : information security, security, iso, itil, awareness, Information Security Awareness, nist, cobit, cyber security, awareness training, awareness education, cnss, standards, security standards

# BİLGİ GÜVENİLİĞİ FARKINDALIĞININ ÖNEMİ

## ÖZET

Günümüz dünyasında, bilgi güvenliği hayatın her adımında ve her ülkesinde en önemli konudur. Organizasyonlar ve ülkeler, bilgiyi saklayabilmek için birçok kaynak, güç ve para harcamaktadırlar. Bu yüzden, bilgi güvenliğini nasıl korumamız gerektiğini bilmek için, bilginin ne olduğunu ve sistemlerimize nasıl uygulayacağımızı bilmemiz gerekmektedir.

Standartları kullanarak ve iyi bir güvenlik altyapısıyla, her şirket, organizasyon ve hatta sıradan insanlar bile bilgilerini güvende tutabileceklerdir. Ancak, sadece güvenlik programları ve standartlar koruma için yeterli değildir. Aynı zamanda farkındalık eğitimleri ve uygulamaları da çok önemlidir. Çünkü eğer sistemde bir güvenlik programı olsa bile, kullanıcı programı yararlı bir şekilde kullanmayı bilmediği takdirde, tam bir performans elde edilemez. Bundan dolayı, kuruluşlar belirli aralıklarla farkındalık seminerleri düzenlemelidirler.

Bu noktada, Bilgi Güvenliği Farkındalık Programları devreye girmektedir. Bir şirket güvenlik programlarını uyguladığında ve standartları kullandığında, her kişi için bilgi farkındalığı programı hazırlamalıdır. Bu metot ile herkes verileri nasıl koruması gerektiğini öğrenecektir. Uzun süreli farkındalık programlarında, insanlar programı ayrıntılı bir şekilde uygulamayı öğrenirler ve veri korumasında devamlılık sağlanmış olur.

Bu tezde, ilk olarak, bilgi güvenliğinin ne demek olduğu ve hangi standartların kullanılması gerektiği açıklanmıştır. Daha sonra, bilgileri tehlikelerden korumak için kişilerin farkındalıkları, farklı türlerde bilgi güvenliği farkındalığı programı basamakları ve bu metotları nasıl uygulanacağından bahsedilmiştir. Farkındalık metotları için, bazı şirket ve organizasyonların kullandığı yöntemler örnek olarak verilmiştir.

Bu tezde, bazı sektörlerdeki şirketlerin farkındalık programlarını kullanma yüzdeleri bulunmaktadır. Bu bilgi sayesinde, hangi şirket ya da organizasyonların gerçekten verilerini tehlikelerden koruduklarını görebilmekteyiz. Bu sonuç ile kaç şirketin bilgi

güvenliği farkındalık programlarını kullandığını görebilmekteyiz. Bilgi güvenliği programlarıyla ilgili kaç şirketin gerçekten bilgi sahibi olduğunu ve eğer bu programları kullanıyorlarsa hangi metotlardan yararlandıklarını görebiliriz. Bu sonuçlara göre, ülkemiz hakkında da fikir sahibi olabilmekteyiz. Gerçekten tehlikenin farkında mıyız ya da metotları kullanıp bilgiyi koruyabiliyor muyuz?

Bununla beraber, eğer şirketler ya da sıradan kullanıcılar veri koruma hakkında bir şey bilmiyorlarsa bile, bu onların bilgi korumayı öğrenemeyecekleri anlamına gelmez. Geçmişten günümüze, herkes bilgi güvenliği konusunda ilerleme göstermiştir. Her yıl, düzenlenen seminerlerde, birçok şirket, kuruluş ve insan bilgiyi koruma konusunda daha çok şey öğrenmektedirler. Hazırlanacak daha çok bilgi güvenliği farkındalık programı ile daha çok kişi bu konuda birçok şey öğrenecektir. Bundan birkaç yıl sonra, bilgi güvenliği alanındaki büyük boşluk kaybolacaktır.

Öte yandan, tezde, bilgi güvenliğinin neden şirketler için bu kadar önemli olduğu vurgulanmıştır. Bilgi kaybı yüzünden büyük paralarını kaybeden 5 şirketin örnekleri verilmektedir.

Bu tezde, bilgi güvenliği hakkında bazı soruların cevapları verilmiştir. Ve ileriki periyotlarda bilgiyi korumak için neler yapılması gerektiği konusunda bazı fikirler ve bilgi güvenliği farkındalığının neden herkes için önemli olduğu anlatılmaktadır.

Son olarak, Türkiye'de farklı öğrenim durumları ve yerlerindeki insanlar ile "Bilgi Güvenliği Farkındalığı Anketi" uygulanmıştır. Bu uygulama ile kişilerin bilgi düzeyleri ölçülmüştür. Kişiler anket esnasında yeni bilgiler öğrenmişlerdir. Bu anket sayesinde farklı gruplardaki kişilerin bilgi seviyeleri karşılaştırılmıştır.

**Anahtar Kelimeler:** bilgi güvenliği, güvenlik, iso, itil, farkındalık, bilgi güvenliği bilinçlendirmesi, nist, cobit, siber güvenlik, bilinçlendirme uygulamaları, bilinçlendirme eğitimleri, standartlar, güvenlik standartları

# ACKNOWLEDGEMENT

First of all, I want to thank my supervisor Assoc. Prof. Dr. Fatih KOYUNCU, for helping me to prepare this thesis and to choose this topic.

I want to thank my family for their supports. Also, I want to thank my manager for his help.

**2016, 27 January** **Şehnaz Hilal MOĞOL**

# CONTENTS

## ABBREVIATIONS

| | |
|---|---|
| ACM | Association for Computing Machinery |
| ARPA | Advanced Research Project Agency |
| BSI | British Standards Institute |
| CC | Common Criteria |
| CCEVS | Common Criteria Evaluation and Validation Scheme |
| CEO | Closely Held Corporations |
| CFO | Chief Financial Office |
| CIO | Chief Information Officer |
| CISO | The Chief Information Security Officer |
| CNSS | Committee on National Security Systems |
| COBIT | The Control Objectives for Information and related Technology |
| COMPUSEC | Computer Security |
| COMSEC | Communication Security |
| CTO | Chief Technology Officer |
| DES | Digital Encryption Standard |
| DSS | Data Security Standard |
| EAL | Evaluation Assurance Level |
| EMSEC | Emanations Security |
| ETSI | Internet Engineering Task Force |
| FIPS | The Federal Information Processing Standards |
| GE | General Electric |
| ICANN | Internet Corporation for Assigned Names and Numbers |
| IEC | International Electrotechnical Commission |
| IEEE | Institute of Electrical and Electronics Engineers |
| INFOSEC | Information Security |
| IS | Information Security |
| ISA | Information Security Awareness |
| ISACA | Information Systems Audit and Control Association |
| ISATP | Intra-Site Automatic Tunnel Addressing Protocol |
| ISMS | Information Security Management System |
| ISO | International Organization for Standardization |
| ISP | Information Security Protocol |

| | |
|---|---|
| ITGI | IT Governance Instıtute |
| ITIL | The Information Technology Infrastructure Library |
| ITSM | Information Technology Service Management |
| MIT | Massachusetts Institute of Technology |
| MOTD | Message of the day |
| MULTICS | Multiplexed Information and Computing Service |
| NIST | National Institute of Standards and Technology |
| OGC | United Kingdom's Office of Government Commerce |
| PCI | The Payment Card Industry |
| PCI SSC | Payment Card Industry Security Standard Council |
| PDCA | Plan-Do-Check-Act |
| SAT | Security Awareness Training |
| TR | Technical Report |
| TRANSEC | Transmission Security |
| TSK | Türk Silahlı Kuvvetleri |

## LIST OF TABLES

# LIST OF FIGURES

## LIST OF GRAPH

# CHAPTER ONE

## INTRODUCTION

Until now from the past information is always very important in our houses, schools, banks, and offices, every step of our daily life, and even in the war or the peace time in a country. In all areas, information is the first thing that we have to keep in safe for the first place. If the companies, organizations and human do not show the extra attention to the information security, then there are lots of losses coming. In this manner information security is always important in every step of human's life time.

Today, there are no wars in real, but in the technological situations cyber wars are always continue. Every company, organization or country have to keep the important information's in safe. To understand the security and how to keep in safe it, we must know the standards, how we can apply it and how it can continue. If we answer this questions we can keep the data's in safe. So understand the security we start with the history of it.

The first chapter is an introduction of the thesis, the meaning of information security and about the history of information security. This chapter, is also mentioned the supporting concepts and parameters of information security. Second chapter is explain the information security standards. Third chapter is about the explanation of information security awareness. In this chapter also gives some examples for hacking in big companies. Fourth chapter is explain the awareness programs and the importance of information security awareness. In the fourth chapter, there are program and training models are explained. Also Information Security in Turkey is explained in this chapter. In this chapter, there are also survey results which I prepared in three different groups. Through this survey, different level of knowledge of people were observed. Fifth chapter is concludes the thesis. There are some suggestions and advices for the future period.

## 1.1. History of Information Security

Information security is always important in human's life. In the past in the war times countries send information or secret messages about the war or secret treaties with each other, to protect these info's they took security measures. These are not like todays measures but in that time these are very detailed. For example; the courier was younger and athletic, and the messages were encrypted. No one could solve the message without decrypting code. Mentioned in the book of, History of information security: A Comprehensive Handbook, "the protection of communication security depended upon three components: psychology, physical integrity, and encryption."[14]

Using samples from the past, information security issues are always improved. If we talk about from this period; "the need for computer security—that is, the need to secure physical locations, hardware, and software from threats— arose during World War II when the first mainframes, developed to aid computations for communication code breaking (see Figure 1.1.1), were put to use. Multiple levels of security were implemented to protect these mainframes and maintain the integrity of their data."[17]

Several key events contributed to the birth and evolution of computer and network security. The timeline can be started as far back as the 1930s.[3]

The primary threats to security were physical theft of equipment, espionage against the products of the systems, and sabotage. One of the first documented security problems that fell outside these categories occurred in the early 1960s, when a systems administrator was working on an MOTD (message of the day) file, and another administrator was editing the password file. A software glitch mixed the two files, and the entire password file was printed on every output file.[17]

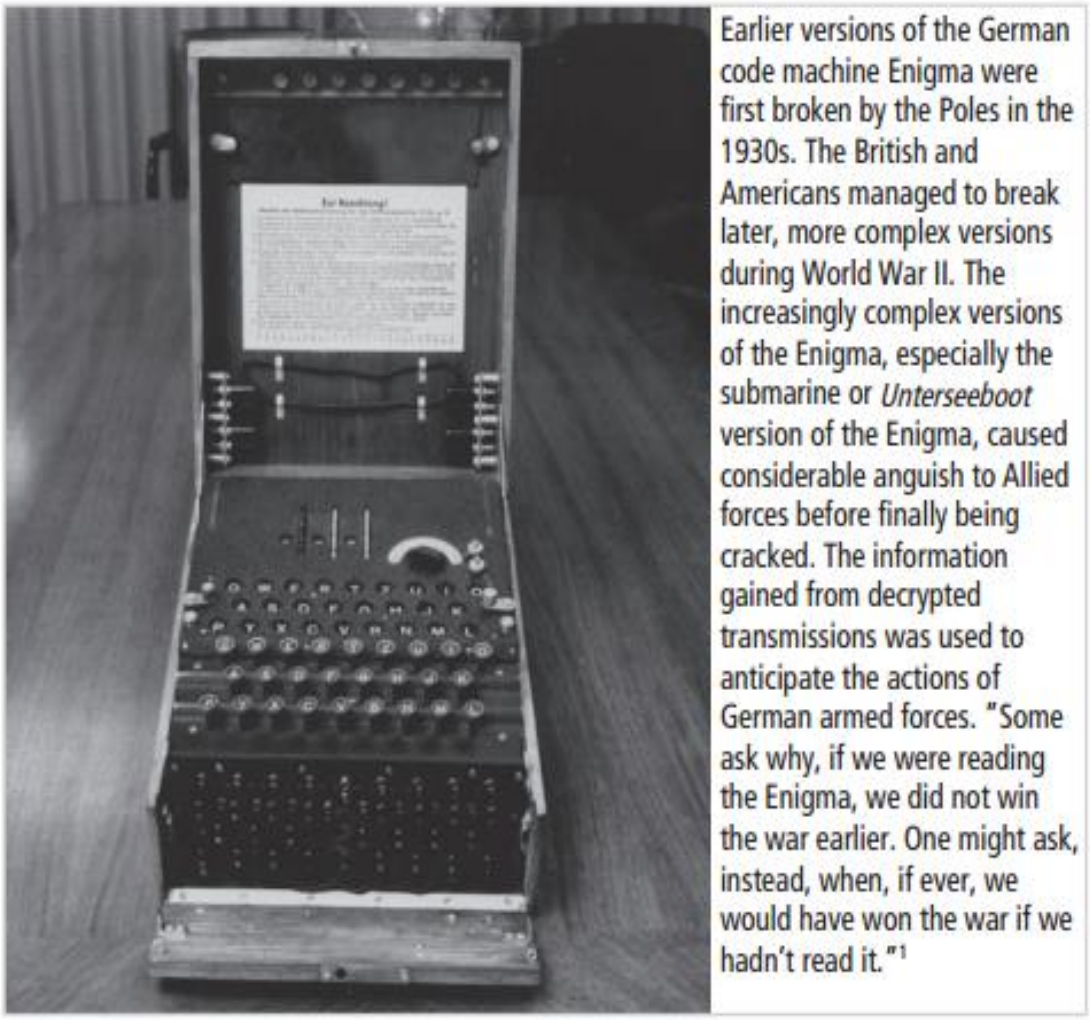



**Figure 1.1.1:** The Enigma [3]

### 1.1.1 The 1960s

In the 1960s, the term "hacker" is coined by a couple of Massachusetts Institute of Technology (MIT) students.[3]

The Department of Defense's Advanced Research Project Agency (ARPA) began examining the feasibility of a redundant, networked communications system to support the military's exchange of information. Larry Roberts, known as the founder of the Internet, developed the project—which was called ARPANET—from its inception. ARPANET is the predecessor to the Internet (see Figure 1.1.2.1) for an excerpt from the ARPANET Program Plan) file.[17]

### 1.1.2 The 1970s and 80s

In December of 1973, Robert M. "Bob" Metcalfe, who is credited with the development of Ethernet, one of the most popular networking protocols, identified fundamental problems with ARPANET security. Individual remote sites did not have sufficient controls and safeguards to protect data from unauthorized remote users. Other problems abounded: vulnerability of password structure and formats; lack of safety procedures for dial-up connections; and nonexistent user identification and authorization to the system. Phone numbers were widely distributed and openly publicized on the walls of phone booths, giving hackers easy access to ARPANET. Because of the range and frequency of computer security violations and the explosion in the numbers of hosts and users on ARPANET, network security was referred to as network insecurity. In 1978, a famous study entitled "Protection Analysis: Final Report" was published. It focused on a project undertaken by ARPA to discover the vulnerabilities of operating system security. For a timeline that includes this and other seminal studies of computer security, see Figure 1.1.2.1.[17]

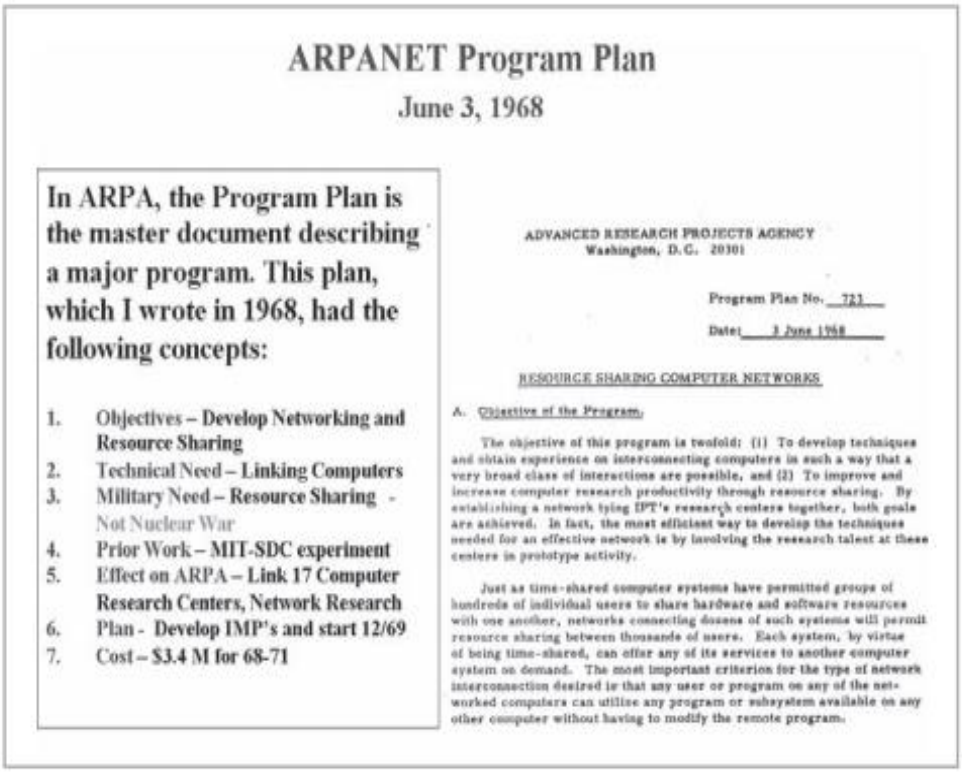



**Figure1.1.2.1:** Development of the ARPANET Program Plan[17]

The security—or lack thereof—of the systems sharing resources inside the Department of Defense was brought to the attention of researchers in the spring and summer of 1967. At that time, systems were being acquired at a rapid rate and securing them was a pressing concern for both the military and defense contractors.[17]

In June of 1967, the Advanced Research Projects Agency formed a task force to study the process of securing classified information systems. The Task Force was assembled in October of 1967 and met regularly to formulate recommendations, which ultimately became the contents of the Rand Report R-609. The Rand Report R-609 was the first widely recognized published document to identify the role of management and policy issues in computer security. It noted that the wide utilization of networking components in information systems in the military introduced security risks that could not be mitigated by the routine practices then used to secure these systems. This paper signaled a pivotal moment in computer security history—when the scope of computer security expanded significantly from the safety of physical locations and hardware to include the following:[17]

- Securing the data
- Limiting random and unauthorized access to that data
- Involving personnel from multiple levels of the organization in matters pertaining to information security

In mid-1969, not long after the restructuring of the MULTICS project, several of its developers (Ken Thompson, Dennis Ritchie, Rudd Canaday, and Doug McIlro) created a new operating system called UNIX.[17]

During the 1970s, the Telnet protocol was developed. This opened the door for public use of data networks that were originally restricted to government contractors and academic researchers.[3]

During the 1980s, the hackers and crimes relating to computers were beginning to emerge. The 414 gang are raided by authorities after a nine-day cracking spree where they break into top-secret systems. The Computer Fraud and Abuse Act of 1986 was

created because of Ian Murphy's crime of stealing information from military computers.[3] In Table 1.2.1 key dates for seminal works in early computer security is shown.

**Table 1.2.1:** Key Dates for Seminal Works in Early Computer Security[12]

| Date | Documents |
|---|---|
| 1968 | Maurice Wilkes discusses password security in Time-Sharing Computer Systems. |
| 1973 | Schell, Downey, and Popek examine the need for additional security in military systems in "Preliminary Notes on the Design of Secure Military Computer Systems." |
| 1975 | The Federal Information Processing Standards (FIPS) examines Digital Encryption Standard (DES) in the Federal Register. |
| 1978 | Bisbey and Hollingworth publish their study "Protection Analysis: Final Report," discussing the Protection Analysis project created by ARPA to better understand the vulnerabilities of operating system security and examine the possibility of automated vulnerability detection techniques in existing system software. |
| 1979 | Morris and Thompson author "Password Security: A Case History," published in the Communications of the Association for Computing Machinery (ACM). The paper examines the history of a design for a password security scheme on a remotely accessed, time-sharing system. |

| | |
|---|---|
| 1979 | Dennis Ritchie publishes “On the Security of UNIX” and “Protection of Data File Contents,” discussing secure user IDs and secure group IDs, and the problems inherent in the systems. |
| 1984 | Grampp and Morris write “UNIX Operating System Security.” In this report, the authors examine four “important handles to computer security”: physical control of premises and computer facilities, management commitment to security objectives, education of employees, and administrative procedures aimed at increased security |
| 1984 | Reeds and Weinberger publish “File Security and the UNIX System Crypt Command.” Their premise was: “No technique can be secure against wiretapping or its equivalent on the computer. Therefore no technique can be secure against the systems administrator or other privileged users … the naive user has no chance.” |

### 1.1.3 The 1990s

At the close of the twentieth century, networks of computers became more common, as did the need to connect these networks to each other. This gave rise to the Internet, the first global network of networks. The Internet was made available to the general public in the 1990s, having previously been the domain of government, academia, and dedicated industry professionals. The Internet brought connectivity to virtually all computers that could reach a phone line or an Internet-connected local area network (LAN).[17]

### 1.1.4 2000 to Present

Today, the Internet brings millions of unsecured computer networks into continuous communication with each other. The security of each computer’s stored information

is now contingent on the level of security of every other computer to which it is connected. Recent years have seen a growing awareness of the need to improve information security, as well as a realization that information security is important to national defense. The growing threat of cyber-attacks have made governments and companies more aware of the need to defend the computer-controlled control systems of utilities and other critical infrastructure. There is also growing concern about nation-states engaging in information warfare, and the possibility that business and personal information systems could become casualties if they are undefended.[17]

## 1.2. What is Information Security?

In this thesis one of the main topic is “what is security”. Security means that to secure data from a danger or an attack from outside. “How we can protect the information from the outsource risks?”, “Which ways can use in information security?”

Information security, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. The aim of the information security is to protect the information. Information Security is a process. An information systems Security Policy is a well-defined and documented set of guidelines that describes how an organization manages, protects its information assets and makes future decisions about its information systems security infrastructure.[20]

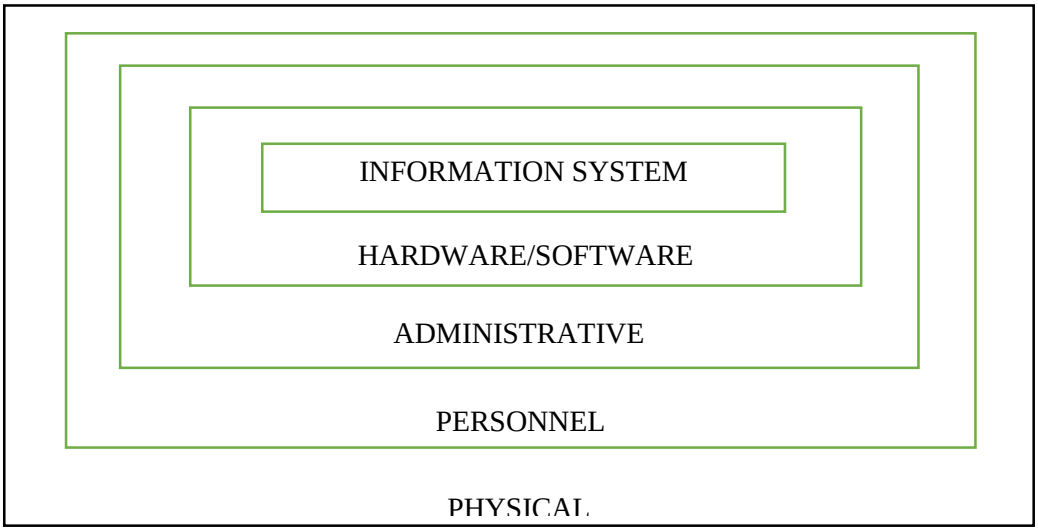



**Figure 1.2.1:** Layers of information security

A good information security program involves two major elements;

- Risk analysis
- Risk management

In the risk analysis phase, an inventory of all information systems is taken. For each system, its value to the organization is established and the degree to which the organization is exposed to risk is determined. Risk management, on the other hand, involves selecting the controls and security measures that reduce the organization's exposure to risk to an acceptable level. To be effective, efficient and reflect common sense, risk management must be done within a security framework where information security measures are complemented by computer, administrative, personnel and physical security measures**.**[12] In Figure 1.2.1, we can see the layers of information security in general form.

The formal definition of information security relies on two sets of parameters:[7]

- Threats, Vulnerability, Assets and Residual risk
- Availability, Integrity and Confidentiality

### 1.2.1. Asset

An asset is anything to which an individual or an organization assigns value. Of specific relevance to information security, all of the following fall into the category of "asset": documents, data, databases, software, physical information technology assets (computers, networks, etc.), proprietary processes, industry specific exclusive knowledge, reputation and image. The valuation of such assets constitutes an essential part of any approach to information security.[7]

### 1.2.2. Residual Risk

For a given set of assets, vulnerabilities and threats, it is possible to assess the risk that these assets will be damaged or compromised.[7]

### 1.2.3. Availability

This is defined as the property of a system (or of a specific system resource) to be accessible and usable whenever required by an authorized entity and according to performance specifications appropriate to the system.[7]

### 1.2.4. Integrity

This is defined as the property that data has not been changed, destroyed or lost in an unauthorized or accidental manner. In practice, there are additional aspects to integrity, dealing with the confidence in data values and the information these values represent (correctness integrity) and with the trustworthiness of the source of the values (source integrity). [7]

### 1.2.5. Confidentiality

This is defined as the property that information (or data) is not made available or disclosed to unauthorized individuals, entities or processes. Techniques, such as encryption, are used to obscure the contents of information and data from parties who do not have access to decryption facilities.[7]

## 1.3. Supporting Concepts of Information Security

### 1.3.1. InfoSec

INFOSEC (Information Security), protect and defense against the information and information systems, from unauthorized entry, modification of information, and exclusion of services by unauthorized users.[9]

INFOSEC, includes all the components constituting of information. These are;[9]

- Hardware /software functions
- Administrative
- Physical structures and devices
- Personnel and communication controls that keep in a reasonable risk for the infrastructure, data and information in the infrastructure.

### 1.3.2. Comsec

COMSEC (Communication Security), to protect communications media, technology, and content. Definition of COMSEC includes four components:[9]

- EMSEC (Emanations Security), the control of internal information leaks to reduce danger.
- Electronic Security, are the measures taken for the protection from unauthorized parties that can be derived from electromagnetic radiation and capture of knowledge.
- TRANSEC (Transmission Security), degradation and protection against deception by imitating, transmission and traffic analysis.
- Cryptographic Security, using cryptographic for protect content of communication.

### 1.3.3. Tempest

TEMPEST is the name of a technology involving the monitoring (and shielding) of devices that emit electromagnetic radiation (EMR) in a manner that can be used to reconstruct intelligible data.[9]

### 1.3.4. Compusec

COMPUSEC (Computer Security) is a military term used in reference to the security of computer system information. Today, it can relate to either the military or civilian community. COMPUSEC also concerns preventing unauthorized users from gaining entry to a computer system.[9]

# CHAPTER TWO

## INFORMATION SECURITY STANDARDS

### 2.1. Standards of Information Security Standards

There are several types of standards that can be used in information security for applying to the system. (see Table 2.1.1) These are;

**Table 2.1.1:** Standards of Information Security

| NAME | SOURCE | DATE | NECESSITY |
|---|---|---|---|
| COBIT | ISACA | 1996 | NO |
| ITIL | International | 1989 | NO |
| NIS SP 800/30 | NIST | 2002 | NO |
| ISO 1335-2<br>(ISO 27005) | Guidelines for Management of IT Security | 1996 | Standard |
| ISO 15408 | Common Criteria | 1996 | Certificate |
| ISO 27001 | New version of<br>BS 7799-2 | 2005 | Certificate |
| ISO 27002 | New version of 17799 and 7799-1 | 2007 | Standard |

### 2.1.1 ISO Standards

#### *2.1.1.1. ISO/IEC 27002:2005 (Code of Practice for Information Security Management)*

ISO/IEC 27002:2005 (replaced ISO/IEC 17799:2005 in April 2007) is an international standard that originated from the BS7799-1, one that was originally laid down by the British Standards Institute (BSI). ISO/IEC 27002:2005 refers to a code of practice for information security management, and is intended as a common basis and practical guideline for developing organizational security standards and effective management practices.[2]

Standard ISO 17799 was merged into ISO 27002 at the beginning of 2007 without making any changes to its contents in order to underscore the fact that it belongs to the ISO- 2700x series of standards.[5]

This standard contains guidelines and best practices recommendations for these 10 security domains: (a) security policy; (b) organization of information security; (c) asset management; (d) human resources security; (e) physical and environmental security; (f) communications and operations management; (g) access control; (h) information systems acquisition, development and maintenance; (i) information security incident management; (j) business continuity management; and (k) compliance.[5]

#### *2.1.1.2. ISO/IEC 27001:2005 (Information Security Management System - Requirements)*

Due to the complexity of information technology and the demand for certifications, numerous manuals, standards and national norms for information security have emerged over the past several years. The ISO 27001 "Information Technology – Security Techniques – Information Security Management Systems Requirements Specification" is the first international standard for management of information security that also allows certification. ISO 27001 provides general recommendations on around ten pages for, among other things, the introduction, operation, and improvement of a documented information security management system that also takes the risks into account. The controls from ISO/IEC 27002 are referred to in a

normative annex. The readers however, are not provided with any assistance for the practical implementation.[5]

#### *2.1.1.3. ISO/IEC 15408 (Evaluation Criteria for IT Security)*

The international standard ISO/IEC 15408 is commonly known as the "Common Criteria" (CC). It consists of three parts: ISO/IEC 15408-1:2005 (introduction and general model), ISO/IEC 15408-2:2005 (security functional requirements) and ISO/IEC 15408-3:2005 (security assurance requirements). This standard helps evaluate, validate, and certify the security assurance of a technology product against a number of factors, such as the security functional requirements specified in the standard.[2]

Hardware and software can be evaluated against CC requirements in accredited testing laboratories to certify the exact EAL (Evaluation Assurance Level) the product or system can attain. There are 7 EALs: EAL1 - Functionally tested, EAL2 - Structurally tested, EAL3 - Methodically tested and checked, EAL4 - Methodically designed, tested and reviewed, EAL5 - Semi-formally designed and tested, EAL6 - Semi-formally verified, designed and tested, and EAL7 - Formally verified, designed and tested. A list of accredited laboratories as well as a list of evaluated products can be found on the Common Criteria portal. The list of products validated in the USA can be found on web-site of the Common Criteria Evaluation and Validation Scheme for IT Security (CCEVS).[2]

#### *2.1.1.4. ISO/IEC 13335 (IT Security Management)*

ISO/IEC 13335 was initially a Technical Report (TR) before becoming a full ISO/IEC standard. It consists of a series of guidelines for technical security control measures:[2]

a) ISO/IEC 13335-1:2004 documents the concepts and models for information and communications technology security management.

b) ISO/IEC TR 13335-3:1998 documents the techniques for the management of IT security. This is under review and may be superseded by ISO/IEC 27005.

c) ISO/IEC TR 13335-4:2000 covers the selection of safeguards (i.e. technical security controls). This is under review and may be superseded by ISO/IEC 27005.

d) ISO/IEC TR 13335-5:2001 covers management guidance on network security. This is also under review, and may be merged into ISO/IEC 18028-1, and ISO/IEC 27033.

### 2.1.2. Cobit

COBIT (Control Objectives for Information and related Technology) describes a method for controlling the risks arising from the use of IT to support business-related processes. The COBIT documents are issued by the IT Governance Institute (ITGI) of the Information domains Audit and Control Association (ISACA). During the development of COBIT, the authors based their ideas on the existing standards for security management such as ISO 27002.[5]

COBIT 4.1 consists of 7 sections, which are (1) Executive overview, (2) COBIT framework, (3) Plan and Organize, (4) Acquire and Implement, (5) Deliver and Support, (6) Monitor and Evaluate, and (7) Appendices, including a glossary. Its core content can be divided according to the 34 IT processes.[2]

### 2.1.3. Itil (Or Iso/Iec 20000 Series)

The IT Infrastructure Library (ITIL) is a collection of several books on the subject of IT service management. They were developed by the United Kingdom's Office of Government Commerce (OGC). ITIL concerns the management of IT services from the point of view of the IT service provider. The IT service provider could be an internal IT department as well as an external service provider. The overall goal is to optimize and improve the quality and cost-effectiveness of IT services.[5]

An ITIL service management self-assessment can be conducted with the help of an online questionnaire maintained on the website of the IT Service Management Forum. The self-assessment questionnaire helps evaluate the following management areas: (a) Service Level Management, (b) Financial Management, (c) Capacity Management, (d)

Service Continuity Management, (e) Availability Management, (f) Service Desk, (g) Incident Management, (h) Problem Management, (i) Configuration Management, (j) Change Management, and (k) Release Management.[2]

### 2.1.4. Payment Card Industry Data Security Standard

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed by a number of major credit card companies (including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International) as members of the PCI Standards Council to enhance payment account data security. The standard consists of 12 core requirements, which include security management, policies, procedures, network architecture, software design and other critical measures. These requirements are organized into the following areas:[2]

1. Build and Maintain a Secure Network
2. Protect Cardholder Data
3. Maintain a Vulnerability Management Program
4. Implement Strong Access Control Measures
5. Regularly Monitor and Test Networks
6. Maintain an Information Security Policy

### 2.1.5. NIST 800 Standards

#### *2.5.1.1. NIST 800-26*

NIST 800-26 is a popular control standard that many organizations base their security practices. NIST is a no regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's Computer Security Division has developed several standards to improve information systems security that have been widely adopted by both Federal agencies as well as commercial organizations. Rsam's NIST template is based on SP800-26 Security Self-Assessment Guide for Information Technology Systems, SP800-53 Recommended Security Controls for Federal

Information Systems and other related documents. Each assessment area in Rsam is carefully mapped to NIST standards & guidelines, allowing clients to easily conduct an assessment against NIST. The purpose of this NIST 800-3/26 is to provide guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government. The guidelines apply to all components of an information system that process, store, or transmit federal information.[1]

#### *2.5.2.2. NIST SP 800-30*

This document built on the Federal IT Security Assessment Framework (Framework) developed by NIST for the Federal Chief Information Officers Council. The Framework established the groundwork for standardizing on five levels of security status and criteria agencies could use to determine if the five levels were adequately implemented. This document provided guidance on applying the Framework by identifying 17 control areas, such as those pertaining to identification and authentication and contingency planning. In addition, the guide provided control objectives and techniques that could be measured for each area.[13]

An effective risk management process is an important component of a successful IT security program. The principal goal of an organization's risk management process should be to protect the organization and its ability to perform their mission, not just its IT assets. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organization. The SP 800-30 document was created by the National Institute of Standards and Technology and is public domain.[18]

# CHAPTER THREE

## INFORMATION SECURITY AWARENESS

### 3.1. What is Information Security Awareness?

Besides the importance of information security, information security awareness is also so important. While ensuring the security of information, awareness, training and education is always important. (Figure 3.1.1) Without awareness, training and education IS cannot be achieved in full. TO understand the IS and how we can apply IS to this in the organizations, we must start to understand what is information awareness, training, education. According to the Thomas R. Peltier, learning consists of three key elements:[10]

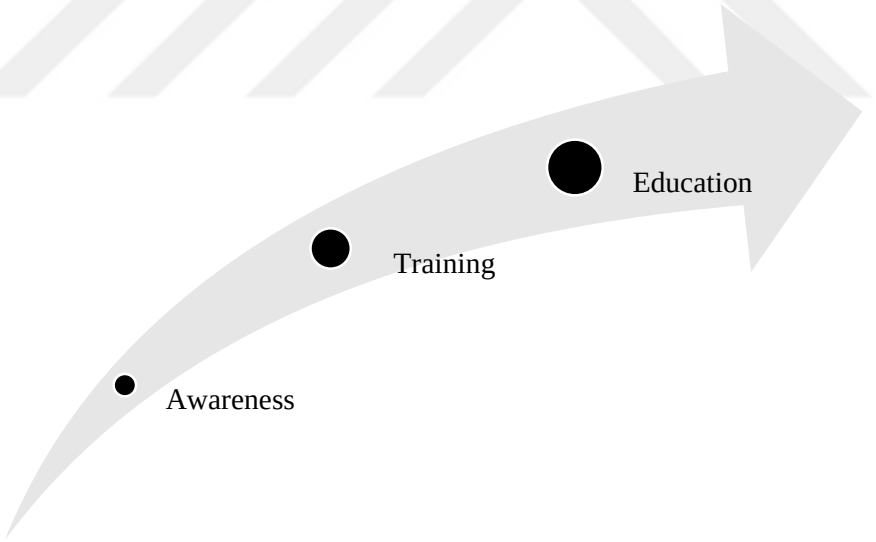



**Figure 3.1.1:** Information Security Model[10]

1. *Awareness*, which is used to stimulate, motivate, and remind the audience what is expected of them.

2. *Training*, the process that teaches a skill or the use of a required tool.

3. *Education,* the specialized, in-depth schooling required to support the tools or as a career development process.

If we look at the various explanations of awareness: Security awareness, is the knowledge and attitude members of an organization possess regarding the protection of the physical and especially, information assets of that organization. According to the European Network and Information Security Agency, 'Awareness of the risks and available safeguards is the first line of defense for the security of information systems and networks.' Awareness is defined in NIST Special Publication 800-16 as follows: 'Awareness is not training. The purpose of awareness presentations is simply to focus attention on security.[21]

Awareness is the bottom of the information security. Without awareness, training and education cannot work. When we can apply the information security to an organization, users must start with awareness.

Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. In awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate the job performance.[21]

To secure the systems in organizations, Information Security Awareness Programs must be applied. By applying this program, systems in the company must secure and the employees aware the outsource dangerous. Nearly every employee within an enterprise is overhead. Even the CEO, CFO, CTO, and CIO are all overhead. However, they have learned what we need to learn, and that is that we all add value to the bottom line of the enterprise.

## 3.2. Information Security Awareness is a Business Need

In today's business environment most of the companies rely on electronically exchanged information. It is a requirement of all the departments to produce and pass information across different departments in a quick and secure manner to support their

business decisions. Information plays an important role in making decisions. Therefore commercial companies and even the government departments have different classification of data based on its importance and use.[8]

Awareness program basically helps, set measures and educate users on how to behave and get benefit out of information without jeopardizing its confidentiality, integrity and availability. "The employees are the primary users of the information. A lack of awareness and mishandling of information could expose this information to competitors or get corrupted. If this information is freely available the following could be some of the impacts on the company and its business functions:"[8]

- The information available easily can be used by competitors to design strategies and launch new products with more features
- The company's credibility can be affected from this disclosure
- Customer confidence can be lost
- Help competitors to gain more share in the market
- Suppliers and partner would be conscious to deal with the company
- Noncompliance to government and industry laws and standards
- Employees will lose trust and will look for other opportunities

## 3.3. Five Corporate Looses due to Hacking

As we mentioned before Information Security Awareness is so important for all types of companies. ISATP is also important to educate the employees in the company. If there is a big hole in the security and have ignorant employees about IS, this company have a big risk to lose big money and reputation.

Recent reports showed hackers earned $12.5 billion in 2011, mainly by spamming, phishing, and online frauds. Some companies have made their financial losses public, while others chose not to disclose them. Here's a top 5 of the declared losses caused by hackings from last year until present. Undeclared losses may even exceed these ones.[4]

### 3.3.1. $171 Million – Sony

Hacked in April to June 2011, Sony is by far the most famous recent security attack. After its Playstation network was shut down by LulzSec, Sony reportedly lost almost $171 million. The hack affected 77 million accounts and is still considered the worst gaming community data breach ever. Attackers stole valuable information: full names, logins, passwords, e-mails, home addresses, purchase history, and credit card numbers.[4]

### 3.3.2. $2.7 Million – Citigroup

Hacked in June 2011, Citigroup was not a difficult target for hackers. They exploited a basic online vulnerability and stole account information from 200,000 clients. Because of the hacking, Citigroup said it lost $2.7 million. Just a few months before the attack, the company was affected by another security breach. It started at Epsilon, an email marketing provider for 2,500 large companies including Citigroup. Specialists estimated that the Epsilon breach affected millions of people and produced an overall $4 billion loss.[4]

### 3.3.3. $2 Million – Stratfor

Last Christmas wasn't so joyful for Stratfor Global Intelligence. Anonymous members hacked the US research group and published confidential information from 4,000 clients, threatening they could also give details about 90,000 credit card accounts. The hackers stated that Stratfor was *"clueless…when it comes to database security".* According to the criminal complaint, the hack cost Stratfor $2 million.[4]

### 3.3.4. $2 Million – AT&T

The US carrier was hacked last year, but said no account information was exposed. They said they warned one million customers about the security breach. Money stolen from the hacked business accounts was used by a group related to Al Qaeda to fund terrorist attacks in Asia. According to reports, refunding costumers cost AT&T almost $2 million.[4]

### 3.3.5. $1 Million – Fidelity Investments, Scottrade, E*Trade, Charles Schwab

The most recent declared losses were in a brokerage scam. A Russian national was charged in the US with $1.4 million in computer and hacking crimes. $1 million was stolen from stock brokerages Fidelity Investments, Scottrade, E*Trade, and Charles Schwab. The rest of the money was taken from fraudulent tax refunds, with the stolen identities of more than 300 people.[4]

# CHAPTER FOUR

## AWARENESS PROGRAMS AND IMPORTANCE OF INFORMATION SECURITY AWARENESS

### 4.1. Information Security Awareness Program and Training

The security awareness and training program is a critical component of the information security program. As in mentioned with previous topic, if organizations, companies and other business have not known anything about IS and employees have ignorant about the security knowledge, this company/organization had a big risk and might have lose amount of money, time and reputation. Because of that Awareness programs not for the users. This program include all the employees in the company from CEO to basic users.

Physical Security, Desktop Security, Wireless Network and Security, Password Security, Phishing, Hoaxes, Malware, Viruses, Worms, Trojans, etc. are some of the training topics.

An effective security program must take into account the business objectives and mission of the organization and ensure that these goals are met as safely and securely as possible. Understanding the customer's needs must be the first step in establishing an effective information security program. The awareness program must reinforce these objectives and will make the program more acceptable to the employee base. As important as a set of written policies, standards, and procedures is in defining the architecture of the security program and the infrastructure that supports it, the true fact of the matter is that most employees will not have the time or desire to read these documents. The objective of the awareness program is to take the message to the people. The information security program has five key elements that must be presented to the audience.[10]

1. A process to take the message to the user community to reinforce the concept that information security is an important part of the business process

2. Identification of the individuals who are responsible for the implementation of the security program
3. The ability to determine the sensitivity of information and the criticality of applications, systems and business processes
4. The business reasons why basic security concepts such as separation of duties, need to-know, and least privilege must be implemented
5. That senior management supports the goals and objectives of the information security program

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-50, Building an Information Technology Security Awareness and Training Program, provides guidelines that can help federal departments and agencies meet their information security awareness and training responsibilities defined in FISMA and in Office of Management and Budget (OMB) policy. The publication identifies models for building and maintaining a comprehensive awareness and training program as part of an organization's information security program. NIST SP 800-50 is a companion publication to NIST SP 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model. NIST SP 800-50 works at a higher strategic level and discusses how to build and maintain an information security awareness and training program; NIST SP 800-16 addresses a more tactical level and discusses the awareness-training-education continuum, role-based training, and course content considerations. The learning continuum is shown in Figure 4.1.1. [19]

As in mentioned in ISP in before Security Awareness Training (SAT) include the followings:

- The nature of sensitive material and physical assets they may come in contact with, such as trade secrets, privacy concerns and government classified information
- Employee and contractor responsibilities in handling sensitive information, including review of employee nondisclosure agreements

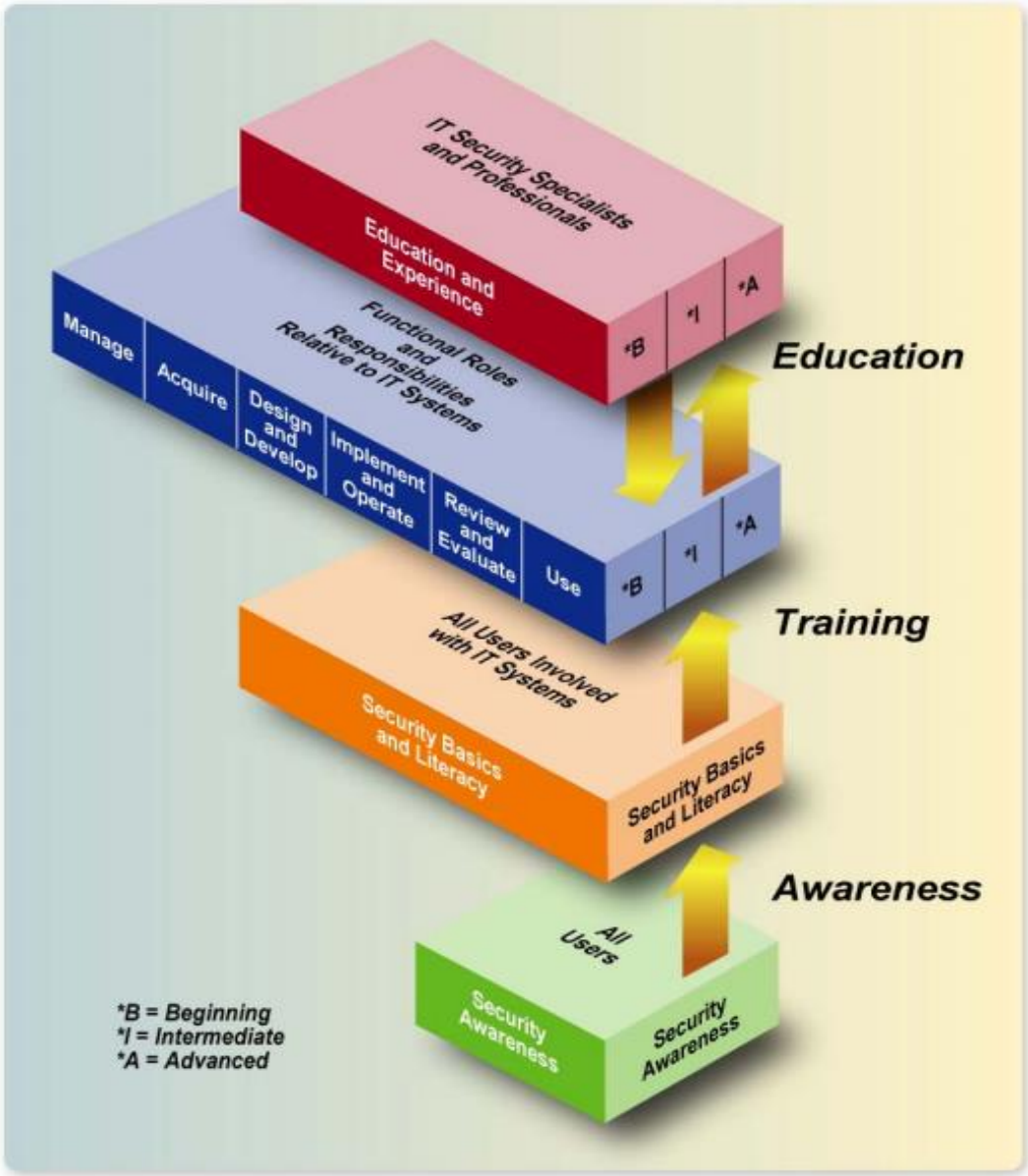



**Figure 4.1.1:** The IT Security Learning Continuum [19]

- Requirements for proper handling of sensitive material in physical form, including marking, transmission, storage and destruction
- Proper methods for protecting sensitive information on computer systems, including password policy and use of two-factor authentication
- Other computer security concerns, including malware, phishing, social engineering, etc.
- Workplace security, including building access, wearing of security badges, reporting of incidents, forbidden articles, etc.

- Consequences of failure to properly protect information, including potential loss of employment, economic consequences to the firm, damage to individuals whose private records are divulged, and possible civil and criminal penalties

Many organizations apply different type of Awareness Programs. According to the Information Security Handbook (the Port Authority of New York & New Jersey 2008, corrected as 2013) in the Security Education and the Awareness Program is basically to provide that all such employees, consultants, third-party contractors, other individuals, entities and/or, where appropriate, third parties develop essential security habits and thereby ensure that all personnel accessing Protected Information understand and carry out the proper handling protocols for those materials. The Chief Information Security Officer (CISO) is responsible for implementing of this training.[11]

The Training Program consists of three interconnected elements: (a) indoctrination training, (b) orientation training, and (c) refresher training, recommended every three years. Each element provides employees, consultants, third-party contractors, and other agency personnel with a baseline of knowledge, as well as periodic updates, about the existing and current Policy.[11]

a. **Indoctrination Training:** Indoctrination Training provides personnel with the fundamentals of the Training Program. It should be completed when beginning employment or assignment to a project for the Port Authority, but no later than sixty (60) days after initial hire, or after commencing work on a project.(..) the general criteria and conditions required in order to be granted a security clearance, procedures for categorizing documents, the obligation to report suspected and alleged policy violations, and the penalties for non-compliance with the policy and for unauthorized disclosure of Protected Information.[11]

b. **Orientation Training:** Orientation Training focuses on the more specific protocols, practices and procedures for individuals whose roles and responsibilities involve reading, using, safeguarding, handling, and disposing of Protected Information.(..) Orientation training should be conducted prior to assignment to a department, project, task, or other special assignment, where

the individual is expected to become involved with receiving and handling Protected Information.(..)[11]

c. **Refresher Training:** Within a three (3) year time period during the anniversary month of the individual's start date on a project, or initial access to Protected Information, all employees, consultants, third-party contractors, and other individuals and/or entities, who continue to have access to sensitive materials, should receive an information security education and awareness training refresher briefing to enhance their information security awareness.[11]

d. **Other Circumstances and Special Briefings:** If a Port Authority employee, consultant, third-party contractor, or other individual and/or entity transfers to another department, is promoted within his or her department, or changes employers on the same project without a break in service, and can provide a record of completion of indoctrination training within the previous twelve months, only annual refresher training may be required. All other situations demand that an individual requiring access to Protected Information fulfill the conditions for information security education and awareness training under this Policy.[11]

And according to the U.S. Department of State Diplomatic Security, The Awareness Team, (Lisa Lindholm, Awareness Branch Chief) in the organizations they use Awareness Program Lifecycle, which is include; Baseline, Develop, Deliver and Measure.(see Figure 4.1.2)[23]

In this Steps:

- Baseline; determining the current state of the situation.
- Develop; crafting and revising the program
- Deliver; Executing the program
- Measure Progress; Determining and reporting results

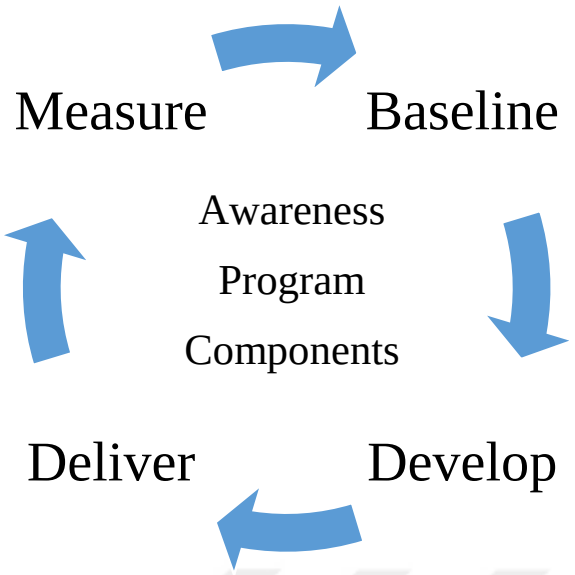



**Figure 4.1.2:** Awareness Program Lifecycle[23]

On the Other Hand, according to NIST, Building an Information Technology Security Awareness and Training Program (October,2003), the awareness and training program may be designed, developed, and implemented in many different ways. Three common approaches or models are described below:[6]

- Model 1: Centralized policy, strategy, and implementation;
- Model 2: Centralized policy and strategy, distributed implementation; and
- Model 3: Centralized policy, distributed strategy and implementation.

The model that is embraced and established to oversee the awareness and training program activity depends on:[6]

- The size and geographic dispersion of the organization;
- Defined organizational roles and responsibilities; and
- Budget allocations and authority.

**Model 1: Centralized Program Management Model (Centralized Policy, Strategy, and Implementation)**

In this model, responsibility and budget for the entire organization's IT security awareness and training program is given to a central authority. All directives, strategy

development, planning, and scheduling is coordinated through this "security awareness and training" authority.[6]

Because the awareness and training strategy is developed at the central authority, the needs assessment – which helps determine the strategy – is also conducted by the central authority. The central authority also develops the training plan as well as the awareness and training material. The method(s) of implementing the material throughout the organization is determined and accomplished by the central authority. Typically, in such an organization, both the CIO and IT security program manager are organizationally located within this central authority.[6]


**Figure 4.1.3:** Centralized Program Management[6]

Communication between the central authority and the organizational units travels in both directions. The central authority communicates the agency's policy directives regarding IT security awareness and training, the strategy for conducting the program, and the material and method(s) of implementation to the organizational units. The organizational units provide information requested by the central authority. For example, to meet its responsibilities, the central authority may collect data on the number of attendees at awareness sessions, the number of people trained on a particular topic, and the number of people yet to attend awareness and training sessions. The organizational unit can also provide feedback on the effectiveness of awareness and training material and on the appropriateness of the method(s) used to implement the material. This allows the central authority to fine-tune, add or delete material, or modify the implementation method(s).[6]

This centralized program management model is often deployed by agencies that:[6]

- are relatively small or have a high degree of structure and central management of most IT functions;
- have, at the headquarters level, the necessary resources, expertise, and knowledge of the mission(s) and operations at the unit level; or
- have a high degree of similarity in mission and operational objectives across all of its components.

**Model 2: Partially Decentralized Program Management Model (Centralized Policy and Strategy; Distributed Implementation)**

In this model, security awareness and training policy and strategy are defined by a central authority, but implementation is delegated to line management officials in the organization. Awareness and training budget allocation, material development, and scheduling are the responsibilities of these officials. The needs assessment is conducted by the central authority, because they still determine the strategy for the awareness and training program. Policy, strategy, and budget are passed from the central authority to the organizational units. Based on the strategy, the organizational units develop their own training plans. The organizational units develop their

awareness and training material, and determine the method(s) of deploying the material within their own units.[6]


**Figure 4.1.4:** Partially Decentralized Program Management[6]

As was the case in the centralized program management model (Model 1), communication between the central authority and the organizational units travels in both directions in this model. The central authority communicates the agency's policy directives regarding IT security awareness and training, the strategy for conducting the program, and the budget for each organizational unit. The central authority may also advise the organizational units that they are responsible for developing training plans and for implementing the program, and may provide guidance or training to the

organizational units so that they can carry out their responsibilities. The central authority may require periodic input from each organizational unit, reporting the budget expenditures made, the status of unit training plans, and progress reports on the implementation of the awareness and training material. The central authority may also require the organizational units to report the number of attendees at awareness sessions, the number of people trained on a particular topic, and the number of people yet to attend awareness and training sessions. The organizational unit may be asked to describe lessons learned, so the central authority can provide effective guidance to other units.[6]

This partially decentralized program management model is often deployed by agencies that[6]

- are relatively large or have a fairly decentralized structure with clear responsibilities assigned to both the headquarters (central) and unit levels;
- have functions that are spread over a wide geographical area; or
- have organizational units with diverse missions, so that awareness and training programs may differ significantly, based on unit-specific needs.

**Model 3: Fully Decentralized Program Management Model (Centralized Policy; Distributed Strategy and Implementation)**

In this model, the central security awareness and training authority (CIO/IT security program manager) disseminates broad policy and expectations regarding security awareness and training requirements, but gives responsibility for executing the entire program to other organizational units. This model normally uses a series of distributed authority directives, driven from the central authority. This normally means creation of a subsystem of CIOs and IT security program managers subordinate to the central CIO and IT security officer.[6]

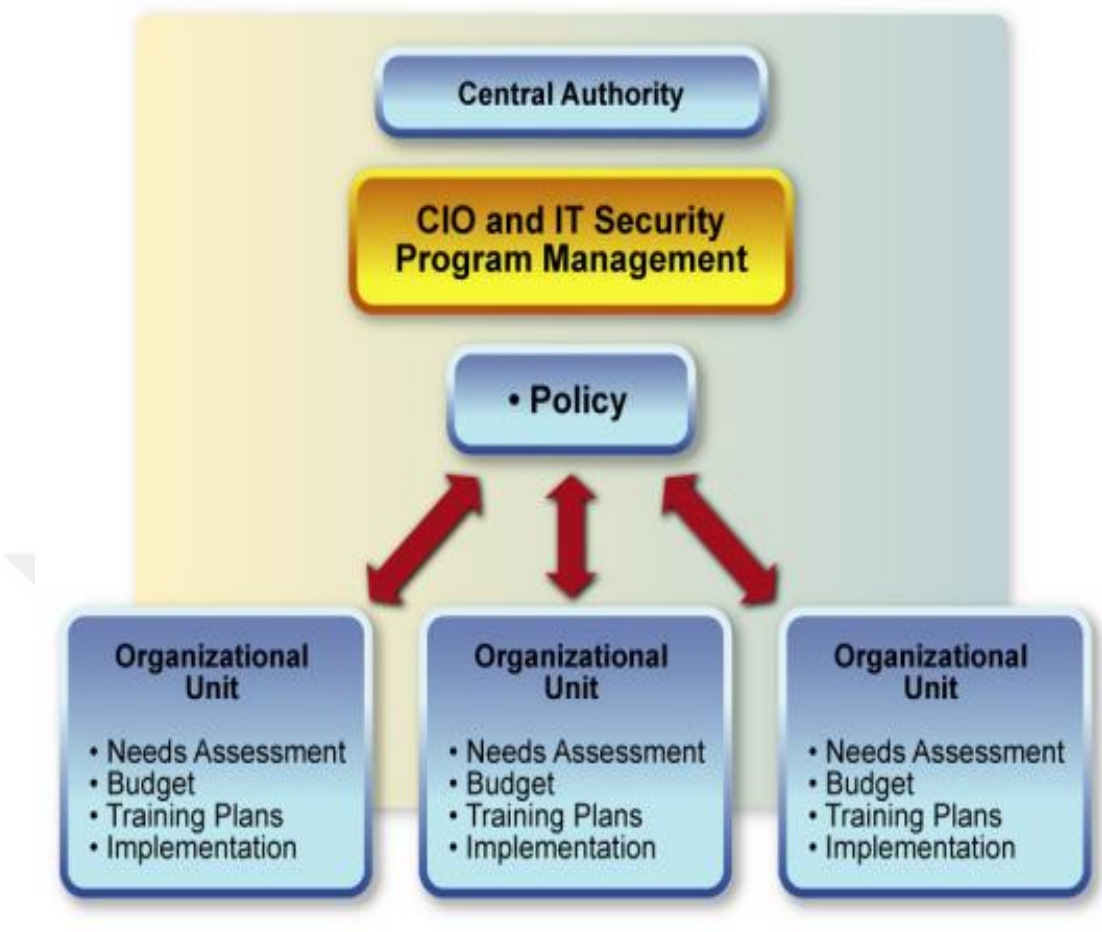



**Figure 4.1.5:** Fully Decentralized Program Management[6]

The needs assessment is conducted by each organizational unit, because in this model, the units determine the strategy for the awareness and training program. Policy and budget are passed from the central authority to the organizational units. Based on the strategy, the organizational units develop their own training plans. The organizational units develop their awareness and training material, and determine the method(s) of deploying the material within their own units. As was the case in the centralized program management model (Model 1) and the partially decentralized program management model (Model 2), communication between the central authority and the organizational units travels in both directions in this model. The central authority communicates the agency's policy directives regarding IT security awareness and training, and the budget for each organizational unit. The central authority may also advise the organizational units that they are responsible for conducting their own needs assessment, developing their strategy, developing training plans, and implementing the

program. The central authority may provide guidance or training to the organizational units so that they can carry out their responsibilities.[6]

The central authority may require periodic input from each organizational unit, reporting the budget expenditures made, the status and results of needs assessments, the strategy chosen by the organizational unit, the status of training plans, and progress reports on the implementation of the awareness and training material. The central authority may also require the organizational units to report the number of attendees at awareness sessions, the number of people trained on a particular topic, and the number of people yet to attend awareness and training sessions. This fully decentralized program management model is often deployed by agencies that[6]

- are relatively large;
- have a very decentralized structure with general responsibilities assigned to the headquarters (central) and specific responsibilities assigned to unit levels;
- have functions that are spread over a wide geographical area; or
- have quasi-autonomous organizational units with separate and distinct missions, so that awareness and training programs may need to differ greatly.

## 4.2. How can be obtained Permanent Awareness

Until now from the past every organizations try to practice permanent awareness with the standards. However, only standards or security programs cannot be useful. If the humans are involved to a work, security programs cannot be efficient at all, because of the wrong usage. If the company or the responsible persons are not involved the awareness education and training, it cannot work in proper way.

There are some ideas that companies can use in the awareness programs;[15]

- Prepare a user guide and give a copy for every person.
- In a regular intervals, prepare Formal or Informal Briefings
- Prepare Security education bulletins and department notices
- Security Awareness Month
- Online Computer-based Tutorials

- Newsletters-The Logon
- Security Awareness Posters and Fliers
- Pick a little brochures to the salary papers.
- Send Reminder mail in a period
- Use posters

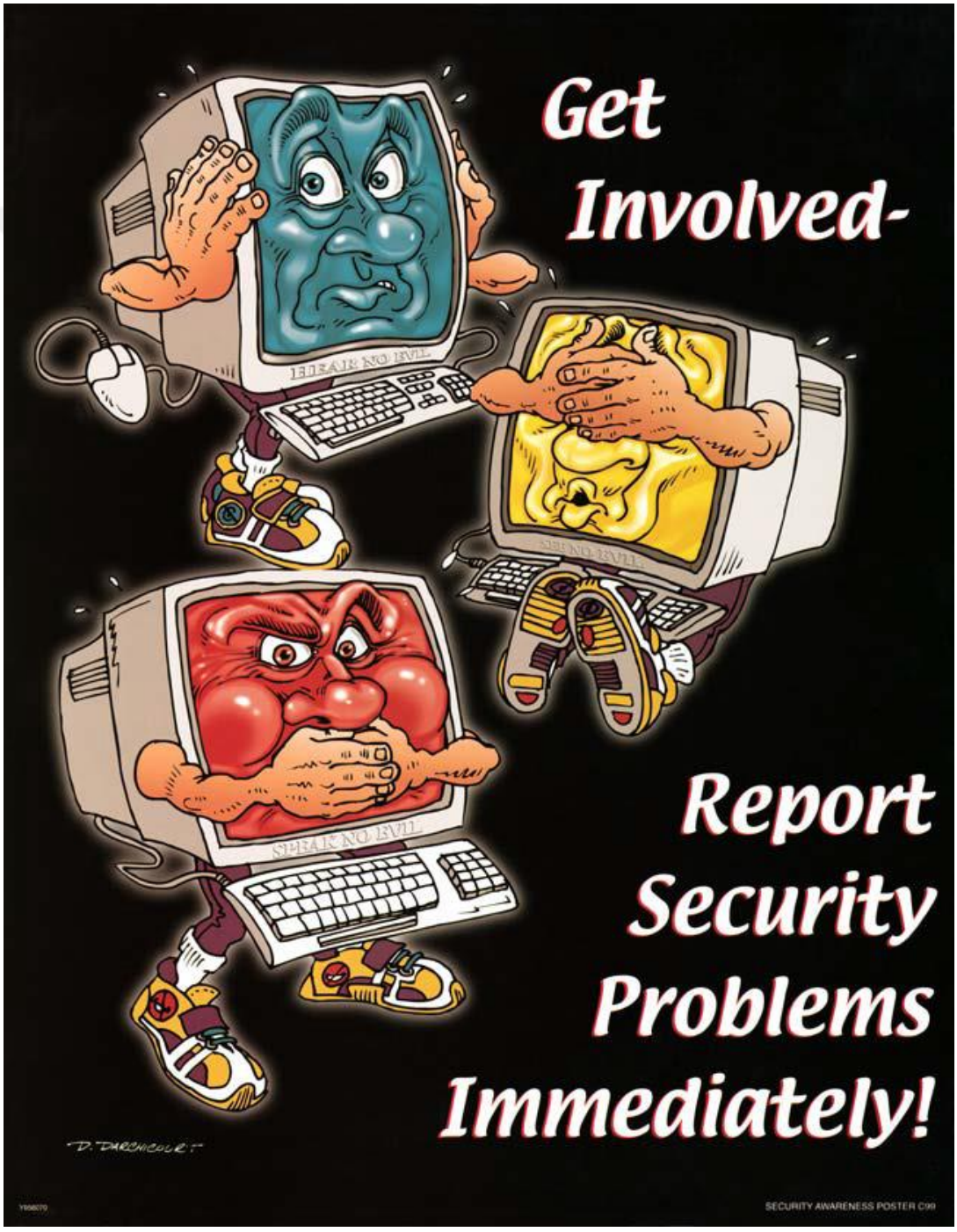



**Figure 4.2.1:** Awareness Poster

- Prepare mini questionnaire
- Give little stickers which have little notes
- Prepare yearly performance reports
- Use screensavers related with security
- Prepare educations about security in a yearly periods
- Prepare little cartoons in the internet about security
- Etc.

These are some trick examples for the awareness programs. By using some of this tricks, employees or regular persons always remember that security is so important and these methods are very important try.

## 4.3. Importance of Information Security Awareness

Because of the importance of information, information security awareness is also important. Today, humans all around the world work with data. If one of them is missing, there is a critical problem in there. Imagine that if you have a big company and you have sign up an contract, at last hours someone steal the data from your company. So your contract are brake down. May be someone steal all information in the hospital. Thus, all the information about patients are gone.

As in these examples, every day organizations, companies even you get several important information that you want nobody learn one of it. Every information is special for somebody. So to protect the information we must teach how to protect them. People must learn which types of dangerous are wander around us.

In this position “Information security awareness” is so important and efficient. With information security awareness, people learn how to protect the data and whish way is useful or what can they do to protect. There are several foundations, which wants to teach the awareness topics. They prepare awareness programs for free for everyone.

According to the general resources and many researches, almost 99% of security programs has broken by using social engineers methods with broke security tests.

Because of that result is not only the security programs. Awareness, education and training with employees and humans are not enough. We cannot provide security with only Security programs or organization methods. Humans are the biggest factor in this case.

In generally, when we control the managements, companies or other stuffs the percentage of the status of Security Awareness is like;

- banking (42.%)
- consulting (5.6%)
- education (92%)
- energy and utilities (13.4%)
- financial services (4.2%)
- government (22.2%)
- healthcare (4.2%)
- legal (7.7%)
- manufacturing (8.5%)
- other (20.4%)

As a result, today the intensive of Information Technology, security should be at the highest point. In the past, war is in the battle area but today cyber security wars between the countries. Countries required the data and knowledge from each other. According to the book of Siber Savaş (Hasan Çifci,2013) " Cyber Security is not only the activity, it is accepted a part of the National Security**.**"[9] As we look at that window, information and the security is the most important thing to keep in safe in the first place in a country. Everyone in the country accepts this fact and get training to keep them in safe. By using Information security Awareness Programs, every human is aware of the topic.

However, only one training or an education program is not useful. Employees or a regular person, who can use pc in their home, are not try to use the safe ways. For this reason little tricks, notes, reminders or similar things are useful to accept and practice the methods. In this manners, companies, education places, security services and the places like that have the biggest responsibilities for prepare awareness programs.

However, despite all this made, many companies haven't use the security programs exactly. Some of them have the security programs, and standards but humans are not aware of what security is or what they can do for a secure pc usage. Companies have really big responsibilities in this area.

The governments are responsible too. Because there are some spaces with the cyber laws. By preparing the laws and educate the organizational structure, we have to cover the right way in information security. After several years, with this organizations, education and awareness programs everyone keeps the data's in safe.

## 4.4. Information Security Awareness in Turkey

In Turkey, Tübitak BİLGEM, Cyber Security Institute, TSK, information security associations, ASELSAN and some other agencies have many organizations for the awareness programs. Organizations prepare symposiums in every year. Many companies participate this organizations. Many speakers join in this symposiums, they share their knowledge with each other.

For example; Tübitak BİLGEM prepared an information system security education catalog in 2015. In this program there are 25 different levels of education section. In these sections there are 4 main levels. These are; entry-level, standard level, advanced level, and upper advanced level.[22] Users must select the levels according to their knowledge levels.

As we see, there are some foundations that prepared awareness programs for users. There are research programs that created in schools or work places about information security.

There is a research which is about "a research on students Information Security Awareness". In this research, analysts worked with 2449 primary and high school students and they got some different results. "Students stated that everything can be easily done by computer and internet, and they can research through the internet and learn more via internet. Moreover they evaluated internet as a communication tool. Students stated that they play both educative and entertaining games and internet supports them to do their homework." (Mehmet Tekerek, Adem Tekerek, A research

on Students' Information Security Awareness, Turkish Journal of Education,2013 pg.8) Also, according to the result of this research "Students' awareness levels are very low in terms of using secure passwords, online secure communication, making malware inspection, document protection, personal computer security, firewall and the use of filtering software, getting friends via internet and whether the internet is a safe space or not."[16]

Despite having these foundations, companies, organizations and programs in Turkey, still there are other companies or users which do not know about information security or awareness trainings. However, with the increase of this programs and researches every time the percentage of to be aware user is increasing.

Many foundations, companies and organizations do not know anything about the information security. Their systems work in basic levels. Systems are just upgrade, the firewalls and antivirus programs are working. And in a period, systems warn users, about change passwords. So there are several information losses came out. However, in recent years, government publish documents about national security plans, awareness plans so, with these documents and declarations, every year awareness foundations are increase.

If the information security awareness programs increase in Turkey, information security and protecting the information also increase.

Preparing the surveys, shows us to see the actual results of "people's knowledge about information security" and "How they pay attention about information security" and "ideas and demands about the information security awareness". According to these ideas, I prepared a survey in three different locations which you can see at the appendix. In these locations, there are three different type of groups which are, public institutions, a university and a high school. In all these groups, ages, education levels, status and capacity of knowledge are different from each other. The purpose of making this survey is to see the level of knowledge, different age, levels and status of the people.

First survey group, consists of public employees. There are hundred person in the group. In generally, the age of the group between 20 and 40. The education levels are different. They work in different departments of the institution. They also work in different positions in the institution.

In the group,

- 47 people can use the internet more than 15 years. 25 people use it 10 to 15 years, 24 people use it among 5 to 10 years. Only 2 person use the internet among 1 to 5 years.

- 35 people use more than 4 electronic devices in their daily life. 59 people use 2 to 4 electronic devices and only 6 person use 1 electronic device in their daily life. It shows us that more than 90 percentage of people can use many electronic devices in daily life. It becomes a daily routine in our life.

  The public employees,

- 61 among 100 say that they have knowledge about information security. 35 people among 100 say that, they know little bit about information security and only 6 person say, they don't know anything about information security. According to these results in the public institution many people aware what information security is? Most of the employee learn the knowledge about information security from internet, trainings, books or documents, and in schools.

- 43 employee among 100 can absolutely agree that the information security is a part of their lives. 49 among 100 can agree the same idea. However 8 of them are not agree that information security is not part of their lives.

- 50 employee say that they get educated about information security in the institution. But other 50 employee say that they don't get educated about information security. It shows us that not all the employee get the trainings. They may not be want to attend the training. As in the previous, 44 people among 100 can get educated how they can protect their data's. And 56 people

among 100 cannot get educated how to protect their data's. In the institution, these numbers must be increased. Thus every employees learned how to protect their information form the dangers. Training and education is the first step, to learn the information security.

The other step is,

- Employees must know that, who is in charge from information security. According to the survey, 75 among 100 know who is in charge. However 23 employee don't know who is responsible from information security in the institution. 2 employee are not interested in who is in charge.

The other question is;

- "For the security of the computer you are using, to which of the following items you pay attention?" The employees say that; 69 employees control the income mails, 82 of employee concern about the passwords, 55 employees backup the information to external memory, 64 employees can use the anti-virus programs, 61 of them can control the sharing personal information. This high percentages shows us that in general all the employees trying to be careful for security for their personal computers.

At the same time,

- 77 employee among 100 cannot use their personal computer in the office. However, 33 of them can use their personal computer at work. This result is a good example actually, using the personal computer in the work may not help us to protect the information. Someone can get the work files at home, employee may not be protect the information in that files.

- 65 among 100 employee think that it will affect other computers of the process that they do on their computer. However 35 of them do not think that it will affect the other computer that they do on their computer.

- Only 5 employee can share their passwords with other employees. 95 employee cannot share their password with other persons. At the same time, 44 among

100 employee change their password bimonthly, 37 among 100 change once in a six month, 8 of them changed in a year and unfortunately 10 employee do not change their password in their computers. In addition, 90 among 100 person say that they received alerts for their account password changes at regular intervals. 10 among 100 say they do not received any alert.

- 78 people use e-mail to exchange data to their computers. 70 of them use external devices, 45 of them use ftp services, 36 people use hard drives and 16 people use phones to exchange data to their computers. Also 57 people sometimes get back up, 24 people rarely get back up their data and 13 people get back up every day. 6 people do not get back up their information from the computer. In these employee group, 65 people cannot take information to their home. 19 people take the information to home one in a month. 7 people take it once in a week and 9 people take information to home in every day.

- 82 people open the attachment in a mail by look who is sending the mail. Other 16 people may open or always open the attachment mail. Only 2 people say that they do not open the attachments in the mails.

The other question in the survey is,

- If you leave from your computer for a lunch or something, how to protect your information. 70 people say they locked their computers, 25 people locked their accounts, 19 people say that they use password screensaver, 10 people close their computers. Also 8 people only close the monıtors and 2 of them do nothing.

Besides,

- 81 employee use the antivirus programs, 7 employee do not use any program and 2 employee do not know about it. However in this situation some personnel use Linux in their computer so they may not need any antivirus programs as well. Also in connection with this questions, 86 people knows that their

antivirus program is updated. 13 people do not know about it and one of them is not updated. In the other question 76 people scan their files and data with these programs. 22 people do not scan their file and data. 2 people do not know anything about it.

According to the employees,

- 55 among 100 think that their computer are candidate for hackers. 14 from 100 don't think that their computer are candidate. And 31 among 100 do not know is it candidate for hackers or not. But everyone must know that every computer is candidate for hackers. Because every information may important for hackers.

In the survey,

- One of the question is that, are they know phishing. 54 people say that they know what it mean. 30 people say they do not know. 16 people say that they have no idea what it is.

- 24 among 100, use their personal information in some websites (card number, birthdate, passwords, etc.). 49 people do not use their personal information. And 27 people sometimes use their personal information in the websites. According to the survey many employee have social media accounts in different areas. To share the personal information in every sites hackers may take your information or steal your accounts. Also 59 employee think that there may have information in their computer that concern other people. But 41 employee do not think like that.

In general,

- 48 employee think that their computer is in safe. 26 employee think that their computer is not in safe. And 26 employee don't know if it is safe or not. At the same time, 72 employee know that firewall is open. 20 employee do not know about firewall. 10 employee have no idea about firewall.

- If there is a problem occur in the computer, user must know who to connect. User may lose data or information to connect to the wrong person when a

problem occur. At this point, 95 people know who to connect. 3 people do not know and 2 people think that they are not concerned with this.

- 69 people among 100 employee know that automatic update is open in their computer. 23 employee among 100 know that automatic update isn't open in their computer. 8 employee don't know if it is open or not.

Smartphones are the most popular things nowadays.

- 94 people among 100 employees have a smartphone and 6 of them haven't got one. Within these people, only 24 people use antivirus program in smartphones. 65 people do not use any of it. Also 8 people do not know anything if it is available or not. At the same time 13 employee allow others to use their phones. 59 people do not allow and 28 people sometimes allow others to use their phones.

As we mentioned before, surveys, notes, posters or other notifying documents are so important for information security. One of the survey question,

- Are you see any notifying documents in working areas? And 25 employee say yes. 53 employee say they don't see any of it and 22 say sometimes. 27 employee want information or training about information security. 62 employee don't want any information or training. And 11 employee do not need any of it. 77 employee among 100 say they will join, if there is a seminar or training about information security. 14 employee say they do not need any of it and 9 employee are unstable about seminar or training. However 84 employee among 100 want to see little reminding notes and alerts about information security and how they secure their information. 5 employee don't want any notes or alerts and 11 employee unstable about this topic.

Second survey group, consists of university students. There are 113 students in the group. In generally, the age of the group is between 20 and 30. The education departments and classes are different. In generally Students are from Engineering Faculty. They are in different departments such as; mechanical engineer, industrial

engineering, electric and electronic engineering, computer engineering, material engineering and civil engineering.

- In the group, 76 people can use the internet among 5 to 10 years. 20 people use it 10 to 15 years, 14 people use it among 1 to 5 years. Only 3 person use the internet more than 15 years.

- 90 people use 2 to 4 electronic devices and 22 people use more than 4 electronic devices in their daily life. Only 1 person use 1 electronic device in their daily life.

- The students, 65 people among 113 say, they know little bit about information security. 25 people among 113 say that they have knowledge about information security and 23 people don't know anything about information security. According to this results students are not exactly aware what is information security. Most of the students learn the knowledge about information security from internet, trainings, books or documents, and in schools. Internet is the top rate for learning what information security is.

- 74 students among 113 can agree the information security, the part of their life's. 15 students among 113 can absolutely agree the same idea. However 17 of them is not agree that information security is not part of their lives.

- 106 students say that they don't get educated about information security. But other 7 students say that they get educated about information. It shows us that in the university there are less education or training about information security. It must have increase. So students get more conscious. As in the previous 20 people among 113 can get educated how they can protect their data's. And 93 people from cannot get educated how to protect their data's.

According to the survey,

- 13 among 113 know who is in charge. However 76 students don't know who is responsible from information security in the university. 24 students are not

interested in who is in charge. Student must learn and interest with who is in charge in information security.

The other question is;

- "For the security of the computer you are using, to which of the following items you pay attention?" The students say that; 52 students control the income mails, 94 of students concern about the passwords, 67 students backup the information to external memory, 51 students can use the anti-virus programs, 47 of them can control the sharing personal information. This high percentages show us that in general all the students trying to be careful for security for their personal computers.

At the same time,

- 50 students among 113 cannot use their personal computer in the office. However, 63 of them can use their personal computer at work. 64 among 113 students think that it will affect other computers of the process that they do on their computer. However 47 of them do not think that it will affect the other computer that they do on their computer.

- Only 16 students can share their passwords with other person. 97 students cannot share their password with other persons. At the same time, 15 among 113 students change their password bimonthly, 30 among 113 change once in a six month, 15 of them changed in a year and unfortunately 54 employee do not change their password in their computers. Students must have learn to change their password periodically. And also 53 among 113 person say that they received alerts for their account password changes at regular intervals. 60 among 113 say they do not received any alert.

- 81 students use e-mail to exchange data to their computers. 60 of them use external devices, 10 of them use ftp services, 18 students use hard drives and 31 students use phones to exchange data to their computers. Also 45 students sometimes get back up, 39 students rarely get back up their data and 9 students get back up every day. 21 students do not get back up their information from

the computer. In students group, 28 students cannot take information to their home. 29 students take the information one in a month. 33 people take it once in a week and 21 students take information to home in every day.

- 86 students open the attachment in a mail by look who is sending the mail. Other 19 students may open or always open the attachment mail. Only 8 students say that they do not open the attachments in the mails.

The other question in the survey is,

- If you leave from your computer for a lunch or something, how to protect your information. 30 students say they locked their computers, 9 students locked their accounts, 19 students say that they use password screensaver, 49 students close their computers. Also 14 students only close the monıtors and 7 of them do nothing.

Also,

- 80 students use the antivirus programs, 32 students do not use any program and 1 students do not know about it. Besides, in connection with this questions, 47 students know that their antivirus program is updated. 16 students do not know about it and 30 of them is not updated. In the other question 63 students scan their files and data with these programs. 39 students do not scan their file and data. 10 students do not know anything about it.

According to the survey students,

- 66 among 113 think that their computer are candidate for hackers. 40 among 113 do not think that their computer is candidate. And 26 among 113 do not know is it candidate for hackers or not.

In the survey, one of the question is that,

- Are they know phishing? 12 student say that they know what it mean. 49 students say they do not know. 47 students say that they have no idea what it is.

- 35 people among 113, use their personal information in some websites (card number, birthdate, passwords, etc.). 49 people do not use their personal information. And 29 people sometimes use their personal information in the websites. According to the survey many students have social media accounts in different areas. Also 72 students think that there may have information in their computer that concern other people. But 41 employee do not think like that.

In general,

- 30 students think that their computer is in safe. 48 students think that their computer is not in safe. And 35 students don't know if it is safe or not. At the same time, 63 students know that firewall is open. 41 students do not know about firewall. 9 students have no idea about firewall. 55 students know who to connect. 43 students do not know and 15 students think that they are not concerned with this.

- 73 students among 113 students know that automatic update is open in their computer. 28 students among 113 know that automatic update isn't open in their computer. 12 students don't know if it is open or not.

- 106 among 113 students have a smartphone and 7 of them haven't got one. Within these people, only 29 students use antivirus program in smartphones. 80 students do not use any of it. Also 13 people do not know anything if it is available or not. At the same time 39 students allow others to use their phones. 33 people do not allow and 27 people sometimes allow others to use their phones.

One of the survey question,

- Are you see any notifying documents in working areas? And 18 students say yes. 71 students say they don't see any of it and 22 say sometimes. 27 students want information or training about information security. 71 students don't want any information or training. And 15 students do not need any of it. 51 students among 113 say they will join, if there is a seminar or training about information

security. 33 students say they do not need any of it and 29 students are unstable about seminar or training. However 63 students among 113 want to see little reminding notes and alerts about information security and how they secure their information. 13 students don't want any notes or alerts and 37 students unstable about this topic.

The third survey group consists of high school students. There are 100 students in the group. Student's classes, grades, and sections are all different for each other. The age of this group is between 15 and 19. In the group,

- 84 students can use the internet about 5 to 10 years. 6 students use it 10 to 15 years, 9 students use it about 1 to 5 years. 68 of them use 2 to 4 electronic devices and 29 students use more than 4 electronic devices in their daily life. There are 3 students only use 1 electronic device in their daily life.

- 55 students among 110 say that, they know little bit about information security. There are 23 students say that they have knowledge about information security and 22 students don't know anything about information security. As we understand from this part, the level of knowledge about information security is so decrease. Every teenage use different social media, internet and search, however the average of knowledge is not enough. Generally these students take the information security knowledge on internet, documents, school and training. But the highest percentages are come from internet.

- 60 students can agree the information security, the part of their life's. 12 students can absolutely agree the same idea. However 28 of them is not agree that information security is not part of their lives.

- 72 students say that they don't get educated about information security. But other 28 students say that they get educated about information security. In high schools, there are enough lessons or educations for information security. Only 41 students can get educated how they can protect their data's. But 59 students cannot get educated how to protect their data's.

According to the survey,

- 26 students know who is in charge. However 42 students don't know who is responsible from information security in the university. 32 students are not interested in who is in charge. Student must learn and interest with who is in charge in information security.

For the next question,

- "For the security of the computer you are using, to which of the following items you pay attention?" The students say that; 36 students control the income mails, 86 of students concern about the passwords, 41 students backup the information to external memory, 66 students can use the anti-virus programs, 61 of them can control the sharing personal information. This high percentages show us that in general all the students trying to be careful for security for their personal computers.

At the same time,

- 90 students cannot use their personal computer in the office. Only, 8 of them can use their personal computer at school. 52 among 100 students think that it will affect other computers of the process that they do on their computer. But 47 of them do not think that it will affect the other computer that they do on their computer.

- Only 14 students can share their passwords with other person. 86 students cannot share their password with other persons. At the same time, 14 students change their password bimonthly, 13 change once in a six month, 21 of them changed in a year and unfortunately 53 students do not change their password in their computers. 19 students say that they received alerts for their account password changes at regular intervals. 80 say they do not received any alert.

- 78 students use e-mail to exchange data to their computers. 50 of them use external devices, 13 of them use ftp services, 23 students use hard drives and 49 students use phones to exchange data to their computers. The percentage of using phones are increase in student daily bases. Also 34 students sometimes get back up, 41 students rarely get back up their data and 6 students get back

up every day. 19 students do not get back up their information from the computer. In students group, 68 students cannot take information to their home. 11 students take the information one in a month. 9 people take it once in a week and 9 students take information to home in every day.

Most of the students open the attachment mail by looking who is sending the mail.

- 54 students look whose sending. Other 30 students may open or always open the attachment mail. Only 14 students say that they do not open the attachments in the mails.

- If student leave from your computer for a lunch or something, 28 students say they locked their computers, 28 students locked their accounts, 29 students says that they use password screensaver, 33 students close their computers. Also 10 students only close the monıtors and 13 of them do nothing. 83 students use the antivirus programs, 7 students do not use any program and 10 students do not know about it. Besides, in connection with this questions, 55 students know that their antivirus program is updated. 35 students do not know about it and 10 of them is not updated. In the other question 63 students scan their files and data with these programs. 36 students do not scan their file and data. 64 students do not know anything about it. 42 from 100 think that their computer are candidate for hackers. 25 students do not think that their computer is candidate. And 32 student do not know is it candidate for hackers or not.

In the survey, one of the question is that,

- Are they know phishing? 21 student say that they know what it mean. 22 student says they do not know. 57 student say that they have no idea what it is. 19 student, use their personal information in some websites (card number, birthdate, passwords, etc.). 44 people do not use their personal information. And 37 people sometimes use their personal information in the websites. Also 53 student think that there may have information in their computer that concern other people. But 66 student do not think like that. 49 students think that their computer is in safe. 27 students think that their computer is not in safe. And 24

students don’t know if it is safe or not. At the same time, 47 students know that firewall is open. 33 students do not know about firewall. 20 students have no idea about firewall. 63 people know who to connect. 23 people do not know and 14 people think that they are not concerned with this.

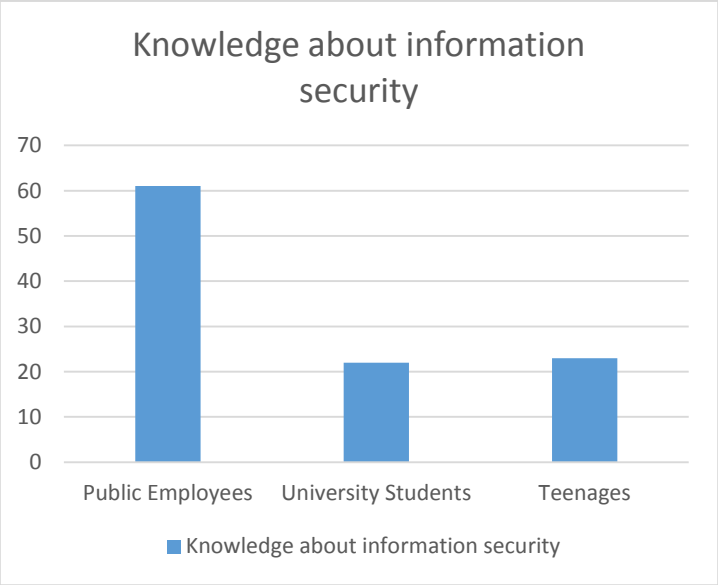
- 66 students know that automatic update is open in their computer. 18 students knows that automatic update isn’t open in their computer. 16 students don’t know if it is open or not.

- 96 students have a smartphone and 4 of them haven’t got one. Within these people, only 46 students use antivirus program in smartphones. 44 people do not use any of it. Also 10 people do not know anything if it is available or not. At the same time 14 students allow others to use their phones. 36 people do not allow and 50 people sometimes allow others to use their phones.

- And 14 students say that are they see any notifying documents in working areas. 66 students say they don’t see any of it and 18 say sometimes. Only, 14 students want information or training about information security. 60 students don’t want any information or training. And 27 students do not need any of it. 43 students say they will join, if there is a seminar or training about information security. 20 students say they do not need any of it and 29 students are unstable about seminar or training. And also 39 students among 100 want to see little reminding notes and alerts about information security and how they secure their information. 13 students don’t want any notes or alerts and 48 students unstable about this topic.

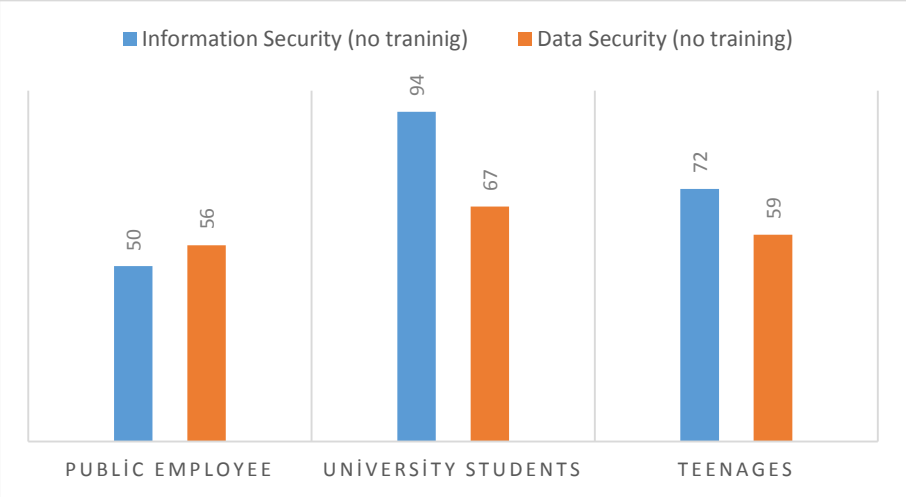
According to this survey, if we discuss all the groups, we have every age range. In public employees mainly use the internet between 5 - 20 years, in university students mainly use between 1-15 years and teenagers mainly use the internet between 5 – 15 years. All three groups use more than 2 electronic devices in their daily life.

Public employees are more conscious than the other two groups. In public employees 61 people know what information security is. However when people become younger their knowledge about information security are decrease.



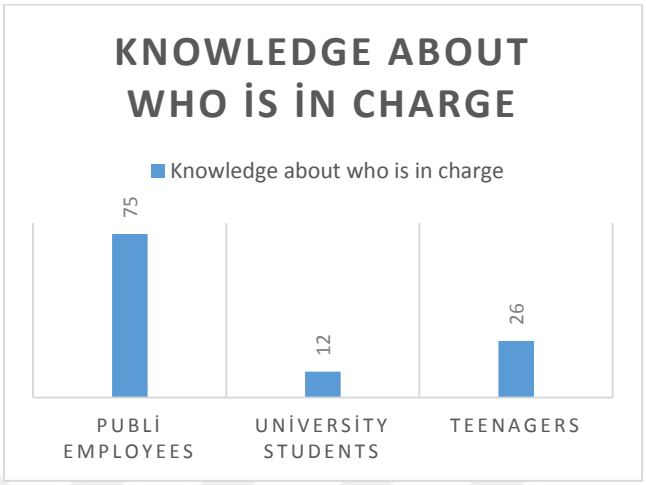

**Graph 4.4.1:** Knowledge about information security

Every group learn information security from internet, school, documents and trainings. Internet is the most preferred from the others. In both three groups, when people become younger, they take less trainings about information security or data security. However in every step of person's life, security always important and in every step people must take trainings about information and data security.



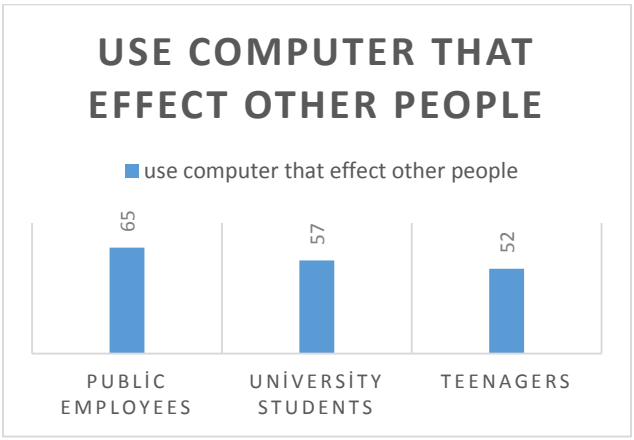

**Graph 4.4.2:** Information security and data security

Also, in three groups, employees are most conscious about knowing who is in charge if there is a problem in their computers. University students and teenagers are less care about this topic.




**Graph 4.4.3:** Knowledge about who is in charge

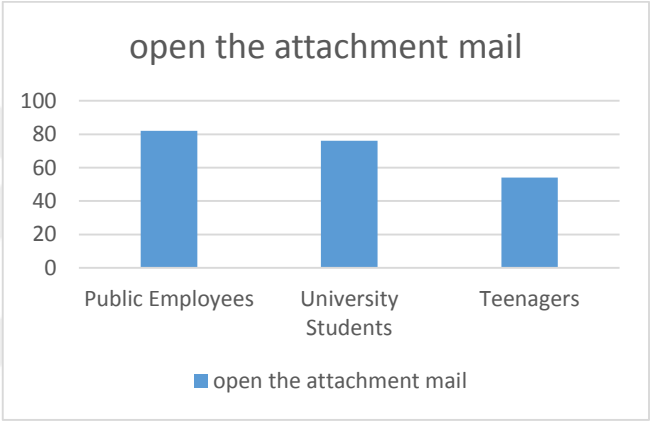
In every group, people are very careful for the following items that protect security of the computer they are using. These are incoming mails, passwords, backup the information to external memory, anti-virus programs, and control the sharing personal information. They both use their personal computers in the office or school. 23 employees use their personal computers and 47 university students use their own computer. Because of their projects and assignments it is more natural that they use their own computers. Another topic is, they all believe that, their usage of computer affect others.




**Graph 4.4.4:** Use computer that effect other people

In three groups member's percentage of sharing their password is very high. Both of them aware the danger about sharing password. In general, most of the employees get alerts about changing their password. The percentage is not high on the other two groups. Both groups use email, external memory, ftp services, phones and usb devices to take the data one to another. Both groups take backups time to time, related with their jobs. Most of the people do not prefer take data to home. In both three groups the percentage of not to take home selection have high percentages.

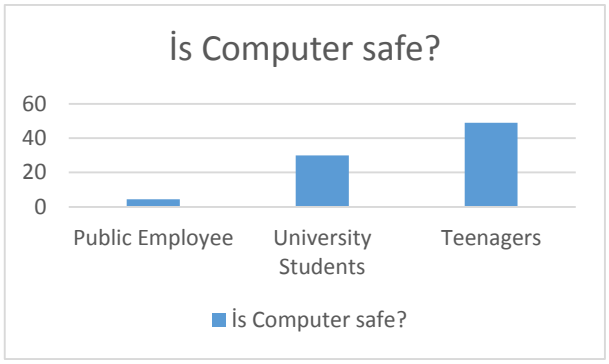
In general, when there is an attachment mail, all group members prefer to open if they know the sender.




**Graph 4.4.5:** Open the attachment mail

They all use antivirus program. Most of the people's programs are updated. In generally they scan incoming data from another person. Employees are more conscious than the other groups. When they become younger the percentage are decrease but not high levels. However, in all groups, member do not think that their computer are candidate for hackers. 54 employee, 12 student and 21 teenagers know that what the phishing is.

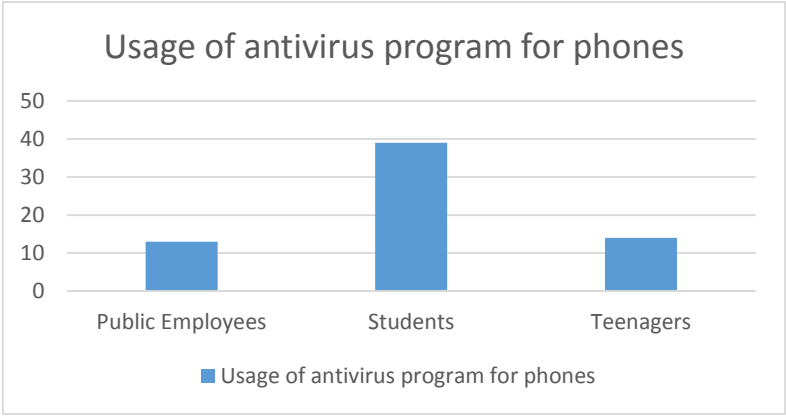
49 employee, 49 student and 44 teenagers do not give their personal information in websites. 72 student, 59 employee and 53 teenager think that they may have any useful information to another person in their computers. However the opposite comment is also high percentage. People think that there are non-information to another person in their own computer but it is not true. Also 49 teenager, 48 employee and 30 student think that their computer is in safe.




**Graph 4.4.6:** Is computer safe?

Employees and students are more conscious than the teenager about the firewall. The percentage of knowing if it is open or not, higher than the teenagers. In generally high level of people know, to contact with responsible person when there is a problem in their system or computers. They also have knowledge about their automatic update is open or not.

Almost all group members use one or more social websites. Because of that result they must know how to protect their information from the out world. Also most of the members use smartphones in their daily life. Generally they do not allow anyone to use their phones. Although, the percentage of using smartphones are high, the usage of antivirus programs are too low. Only 14 teenagers, 13 employees and 39 students use antivirus programs for their devices.




**Graph 4.4.7:** Usage antivirus program for phones

14 teenager, 18 student and 25 employee can see notes, surveys or posters about information security. A few people demand an education or seminars about

information security. 77 employee, 51 students and 43 teenagers want to join, if there is a seminar or training. And also 84 employee, 63 students and 39 teenagers want to dip notes or alerts about information security.

In addition, every group has an idea what is information security and how it affect us. If we look in a general window, people who is working and finish an education life is more conscious than the other groups. Both student groups are in close proximity with each other. As we can see from this survey, students must take classes about information security. If there is no class ever school prepare seminars, trainings. In the working places or education places, surveys, posters, alert notes must be implemented by responsible persons. Thus, information security conscious get bigger in time.

In summary, having mentioned about the general notes and we have the following results and observations:

In the first group,

- Because of using internet for several years generally, many employees know something about information security.
- Employees learn about information security from the internet, documents, books or trainings.
- Many people agree that information security is part of their life. Their jobs affect them to learn that truth.
- However, except this knowledge, they need much more to learn about information security.
- Based on the results, alerts and notes increase the effect of information security awareness.
- In general, many employee do not share their personal information but still many employees share their information with websites.

- They know the general idea of information security but not to exact mean. For example, they use security methods in their daily lives but many of them do not know or not have idea what is phishing.

- Many employees use smartphones. However they have no idea about antivirus programs for phones. They do not protect the information on their phones.

- Trainings are the main way to learn new things for them. They try to attend the trainings for information security, if institution prepare.

In the second group,

- Students ages range are between 20 and 25. These students use 2 to 4 electronic devices in their daily lives.

- Generally, students have a little bit of knowledge about information security. They are learn this knowledge from internet, documents, and books. The effects of school and training is very low.

- Many of the students agree that the information security important for their life. However they have no chance to take any training from school.

- They have no idea that who is responsible from information security in the school.

- They are careful with general topics for protecting their data. Because they generally use their computers at university to for their projects and homework.

- However they are not change their password in a periodic timeline. Less number of students change in a periodic time. One of the reasons for that is, they are not take any alert or notes.

- They open the attachment mails with control from whose sending. They generally take backups of the data's. Many of the students use antivirus programs. Many of them scan their files with this programs.

- In generally in the university, there are no alerts, notes or information which is about information security. Still some of the students share their personal information in websites.

- Many students think that computers are not in safe. Many of them know the details about their computers (firewall, updates, etc.)

- Most of the students do not know anything about phishing.

- Almost all the students use smartphones. However they allow to use their phones from other persons. And generally many of the students do not use antivirus programs in their phones.

- In the university, they say there are no warnings, posters or notes for information security. They are not taking any of trainings for this topic. They are not demand any trainings at all. However if there is a training about this topic many of them wants to join.

In the third group,

- I this group, all the members age range between 15 and 19 and they are all different level classes at the high school.

- Many of them use the internet between 5 to 10 years and use 2 to 4 electronic devices in their daily lives.

- In generally, they say they have knowledge about information security a bit and may be more. They learn the knowledge from school, internet, documents, and books. In these times many high school teach information about information security or how do they protect their information on the websites.

- Many of them agree that information security part of their lives. But still many of them do not know who is responsible from the information security in the school.

- They generally try to protect their data from the outsource dangers. They are not use their personal computers in the school and they do not take data from school to work as well. However, many of them do not believe that what they do in the computer affect the others.

- Many students do not share their password from the others however they do not change the password in a periodical timeline. One of the reason for that, they do not take any alert or warnings for changing their password in a periodical time.

- Students use many ways to transfer the data one to another. Generally they sometimes or rarely backup the data. Many students open the attachment mails by looking whose sending. They generally use antivirus programs. They update their programs and scan the data's with these programs.

- Almost half of them say their computer is in safe but other half of them think not like that. Many of them know t contact the person if there is a problem.

- They use smartphones too and they do not use antivirus programs and protect their data's.

- Low percentages of students say that they cannot see any warning, poster or other stuff about information security. There do not demand any trainings about information security. However they do not take any training at all in the school. If there is a training many of them want to join. And many of them think that it does not matter if there is a warning or information about the information security.

As a result, by using the survey methods we can see the level of knowledge about information security. At these results trainings increase the consciousness about the topic. People learn new methods to protect their information. In these three groups the knowledge and willingness to learn are different. With trainings posters and briefings we can change them.

## 4.5. Organizations that Constitute the Information Security (Cyber Security) Standards

Here are some of the organizations that developed the security standards:[9]

**IEEE (Institute of Electrical and Electronics Engineers):** Developing technical standards.

**ICANN (Internet Corporation for Assigned Names and Numbers):** responsible for the coordination of maintenance and methodology of several databases of unique identifiers related to the namespaces of the Internet, and ensuring the network's stable and secure operation.

**ISO/IEC (Organization for Standardization/International Electrotechnical Commission):** Developing the Information Security Standards.

**ETSI (Internet Engineering Task Force):** Including IP and TCP internet protocol family it has been developing Internet standards.

**NIST (National Instıtute of Standards and Technology):** Promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

**PCI SSC (Payment Card Industry Security Standard Council):** These security standards are developed by the Payment Card Industry Security Standards Council which develops the Payment Card Industry Data Security Standards used throughout the industry.

**CNSS (Committee on National Security Systems):** This is a United States intergovernmental organization that sets policy for the security of the US security systems.

# CHAPTER FIVE

## CONCLUSION

At the beginning of the thesis, we learned that protecting the information is so important for everyone. Today the world was built on to the knowledge. For the first step of the implementing we must understand the importance of security. Without having security, the system does not work properly. After understanding the importance of it, and protecting the data, we can use the standards and security systems. When we apply them, the other step is to educate the people for how to protect the data.

For the education part, information security awareness is also included. In this section, companies must prepare the information security awareness programs to educate the users. In certain period, users should join to the programs. After these, user learn how to keep the data safely. In this way it is not a one-time action, continuity is ensured in the information security.

As in the thesis, applying the surveys for the people show their knowledge about information security. By taking the result of the survey, companies will apply the correct awareness program and training methods for people. Also during the application their knowledge will refresh and they learn the new thing about information security. As the results of the applying survey in this thesis, also we can see the availability of information in Turkey.

If it does not happen in this way, companies, foundations and users may lose very important things and, reputation, etc. So, everyone must be careful for protecting the data and ensure the continuity of the awareness.

In future periods, in order to improve the information security in future, the following precautions can be taken:

- Organizations should held seminars for pay attention.

- All companies should prepare awareness programs for users.
- Government should control the programs.
- Information Security Departments should be established in every company
- Every year all companies must join the security development seminars.
- Information Security Departments should be established in the universities and schools.
- There should be classes and lectures for information security awareness.
- Government should prepare awareness classes and every single person can join training programs for free.

# REFERENCES


[1] Afshin Rezakhani, AbdolMajid Hajebi, Nasibe Mohammadi, *Standardization of all Information Security Management Systems*, March2011, International Journal of Computer Application: (0975-8887), Volume 18, No.8, 5.

[2] *An Overview of Information security Standards*, February 2008, The government of the Hong Kong Special Administrative Region., 5, 7, 8, 9, 10, 11.

[3] Bhavya Daya, *Network Security: History, Importance, and Future*, 3, 4.

[4] Bianca Stanescu, *Top5: Corporate Losses Due to Hacking*, may 17, 2012, 1.

[5] *BSI – Standard 100-1 Information Security Management Systems ISMS*, Bundesamt für Sicherheit in der Informationstechnik, 9, 10, 13.

[6] Mark Wilson, Joan Hash, *Building an Information Technology Security Awareness and Training Program*, October 2003, http://csrc.nist.gov/publications/nistpubs, 22, 23, 24, 25, 26.

[7] Eduardo Gelbstein, Ahmad Kamal, *Information Security*, November 2002, 17, 18, 19, 20.

[8] *Global Information Assurance Certificate Paper*, SANS, 6.

[9] Hasan Çifci, *Her Yönüyle Siber Savaş*, Tübitak Popüler Bilim Kitapları, 2013, 219, 221, 222, 223.

[10] Thomas R. Peltier, *Implementing an Information Security Awareness Program*, CISSP, CISM, 1, 2.

[11] *Information Security Handbook*, The Port Authority of New York& New Jersey, October 15,2008, Corrected as of November 14,2013, 37, 38.

[12] *Information System Security Review Methodology*, EDP Audit Committee International Organizsation Supreme Audir Institutiıon, October 1995, 7.

[13] *IT Law WİKİ*, Nist Speacial Publication 800-26.

[14] Karl Maria Micheal de LEEUW, Jan BERGSTRA ELSEVIER, 2007 The History of Information Security: A Comprehensive Handbook, 2.

[15] Kevin D. Mitnick, William L. Simon, Aldatma Sanatı, ODTÜ yayınları, 238.

[16] Mehmet Tekerek, Adem Tekerek, A research on Students' Information Security Awareness, Turkish Journal of Education, 2013, 8.

[17] Micheal E. Whitman, Herbert J. Mattord, Ptinciples of Information Security.2011., 3, 4, 5, 6, 7, 8.

[18] Network Information Security and Technology News, http://www.nist.org/nist_plugins.

[19] Pauline Bowen, Joan Hash, Mark Wilson, Information Security Handbook: Guide for managers, Information Security, October 2006, 26.

[20] Ted Domopoulos, Article about What is Information Security, Demopoulos Associates.

[21] The new user guide: How to raise information security awareness ENISA, November 2010, 15.

[22] Tübitak Bilgem SGE Siber Güvenlik Enstitüsü, *Bilişim Sistemleri Güvenlik Eğitim Kataloğu*, 2015.

[23] U.S. Department of State Diplomatic Security, http://csrc.nist.gov/organizations, 5, 6.

# APPENDİX A

This survey has been prepared for the thesis titled as “Importance of Information Security Awareness” in Yıldırım Beyazıt University, Graduate School of natural and applied sciences by Şehnaz Hilal MOĞOL under supervision of Assoc. Prof. Dr. Fatih KOYUNCU. The purpose of the survey is to see the level of information for “Information Security Awareness” in different groups of people and determine what can be done.

Advisor Name Surname — Student Name Surname

Assoc. Prof. Dr. Fatih KOYUNCU — Şehnaz Hilal MOĞOL

1. Age: ☐ 15 - 19 ☐ 20 – 25 ☐ 26 – 30 ☐ 30 – 40 ☐ 40 - …

2. Occupation:…….

3. Educational Status: ☐ High School ☐ University ☐ Master Degree ☐ PhD

4. Department: ……5. Class: …….

6. How long have you been using the internet? : ……. (In total year)

7. How many electronic devices do you use, in your daily life? (Laptops, tablets, Pcs, vb.)?

☐ 1 ☐ 2 – 4 ☐ more than 4

8. Do you have the knowledge about the meaning of the Information Security?

☐ Yes

☐ A little knowledge

☐ I do not know

9. Where did you get your information about information security?

☐ School

☐ Internet

☐ Books, documents, papers, etc.

☐ Trainings

10. I see information security as a part of my life.

☐ Strongly agree

☐ I agree

☐ Disagree

☐ Strongly disagree

11. Did you get trainings related to information security, in your location (school, work, etc.)?

☐ Yes ☐ No

12. In your location (work, school, etc.), did you get training about how to protect your data?

☐ Yes ☐ No

13. Do you know who is responsible for information security in your location (work, school, etc.)?

☐ Yes ☐ No ☐ Not interested

14. For the security of the computer you are using, which of the following items you pay attention?

☐ Incoming e-mails

☐ Passwords

☐ Using external memory

☐ Antivirus programs

☐ Backup your data to external memory

☐ Sharing personal information

15. Do you use your personal computers at work?

☐ Yes ☐ No

16. Do you think that, what you do on your computer affect other people?

☐ Yes ☐ No

17. Do you share your password with other people at work/school?

☐ Yes ☐ No

18. How often do you change your password?

☐ Once in two months ☐ Once in a six months ☐ Once in a year ☐ Never

19. Do you get any periodic alert to change your account password at work/school?

☐ Yes ☐ No

20. Which of the following options do you use to exchange data between two computers?

☐ E-mail

☐ External memory

☐ Ftp services

☐ Phone

☐ Hard drives

21. How often do you backup your information?

☐ Every day

☐ Sometimes

☐ Rarely

☐ Never

22. How often do you take information home to work on with your home computer?

☐ Almost every day

☐ At least once a week

☐ At least once a month

☐ Never

23. If someone e-mails you an attachment, how likely are you to open it?

☐ I cannot open

☐ I open, if I know the sender

☐ I sometimes open

☐ I always open

24. When leaving for lunch or to take a break, how do you secure your computer?

☐ I turn off the computer

☐ I lock the computer

☐ I turn off the monitor

☐ I log off

☐ I have a password protected screensaver

☐ None of the above

25. Do you use antivirus program on your computer which you use at work/home?

☐ Yes ☐ No ☐ I don't know

26. Is antivirus program updated which is in your computer in your location?

☐ Yes ☐ No ☐ I don't know

27. Do you scan your files or datas with antivirus programs?

☐ Yes ☐ No ☐ I don't know

28. Are your computers which are used at work/home, candidates for hackers?

☐ Yes ☐ No ☐ I don't know

29. Do you know what phishing is?

☐ Yes ☐ No ☐ I have no idea

30. Do you use your personal information (credit card, date of birth, password and etc.) in websites?

☐ Yes ☐ No ☐ Sometimes

31. Do you think that, are there any information related to the others in your computer at work/school?

☐ Absolutely Yes

☐ Yes, I think

☐ I don’t think so

☐ I absolutely don’t think so

32. Are your computer and information in safe?

☐ Yes, they are

☐ No, they aren’t

☐ I don’t know

33. Do you know that, your firewall turned on or not?

☐ Yes, I know

☐ No, I don’t know

☐ I have no idea

34. Do you know the person to connect when a problem occurs with your computer?

☐ Yes, I know

☐ No, I don’t know

☐ Not interested

35. Are your computer’s automatic updates turned on?

☐ Yes

☐ No

☐ I don’t know

36. Do you use social media websites? İf yes, which one?

☐ I do not use ☐ Facebook ☐ Twitter ☐ LinkedIn ☐ Instagram

☐ Others: ……

37. Do you use smartphones?

☐ Yes ☐ No

38. Do you allow others to use your phone?

☐ Yes ☐ No ☐ Sometimes

39. Do you use antivirus program in your smartphone?

☐ Yes ☐ No ☐ I don’t know

40. Do you see any survey, banner or information about information security at work/school?

☐ Yes

☐ No

☐ Sometimes

41. Have you ever requested any information or training about information security from your work/school?

☐ Yes

☐ Yes, but do not take training

☐ No

☐ I do not need

42. İf there are seminars or training about information security at your work/school, will you join them?

☐ Yes

☐ No

☐ I do not need

☐ Undecided

43. Do you want to be informed about information security with little notes or reminders, at your workplace/school?

☐ Yes

☐ No

☐ It does not matter

# RESUME

**Name and Surname :** Şehnaz Hilal MOĞOL

**Date of Birth :** 16/02/1985

**Birth Place :** Ankara

**Nationality :** Republic of Turkey

**Address :** Sancak Mh. Kahire Cd. 513. Sk Barış Apt. No: 6/2 Çankaya-ANKARA

**E-mail :** msehnazm@gmail.com

**Educational Background:**

- Cyprus International University, Computer Engineering (2009)

**Work Experience :**

- 2011 – 2014: BOTAŞ Doğal Gaz İşletmeleri Bölge Müdürlüğü, Bilgi Sistemleri Müdürlüğü
- 2014 – Still : TRT Genel Müdürlüğü, Bilgi Teknolojileri Dairesi Başkalığı

**Projects :**

- Hospital Automation (Graduation Project)
- Inventory and Demand Automation
- News Guide Web Application
- Archive Automation
- Demand and Distribution Automation
- Image Recording Archive System
- Transmitter Automation

**Language Skills :**

- English : Good
- Chinese : Starter
- French : Starter