International Academic Institute for Science and Technology

International Academic Journal of Science and Engineering
Vol. 2, No. 2, 2015, pp. 31-45.

ISSN 2454-3896

International Academic Journal of Science and Engineering

www.iaiest.com

Assessment of need for attention to the issue of security in usage of Information Technology (Including Case study)

Hamid Gharagozlou[a] , Maryam Mahboobi[b]

[a] *Ph.D. Student of Software Systems, Islamic Azad University, Karaj Branch, Alborz, Iran.*

[b] *Department of Industrial engineering, non-profit institution of higher education, ABA, Abyek, Qazvin, Iran.*

Abstract

Due to the rapid increase in computer data volume and the role of IT in facilitating the exchange of this information today, IT security concept has got a special place among computer users and organizations. On the other hand, the role of human and organizational factors in the realization of this concept will be very important so, the aim of this study is to evaluate the safety of users on using information technology in public use and especially in organizations. To do this cross-sectional study, after compiling a questionnaire which own the reliability and validity, 60 people have randomly selected among all the staffs of Abhar's Department of Education as a case study based on Charles Cochran formula and were asked some questions relate five IT factors including personal computers, e-mail, passwords, antivirus and organizations. After getting the results, to classify responses descriptive statistical methods have used and inferential statistics (Pearson correlation and regression analysis) were used to evaluate the hypothesis of study. The results indicate that there is a significant positive relationship between safety of users and IT factors. Hope this research can helps to institutionalize the culture of suitable protecting of information and attract individuals and organizations' attention to this important issue.

Keywords: security, information technology, IT agents, users, organizations

Introduction:

A unique feature of the new era is innovation and rapid change which is referred to that as the age of information. Organizations in the age of knowledge are facing dynamic compatibility major challenges at all levels. But in the meantime, those organizations which use tools, new technologies and opportunities for their benefit will be successful (Taghipour & et al., 2014). Unlike 25 years ago when working with computer generally accepted by a small number of experts in this field, today hundreds of millions of computers are used for processing any conceivable data by users whose mostly are amateur and connect together by a strong communication network which is named the Internet (Hoonakker et al, 2009). With the spread of the Internet and use it in different dimensions, organizations and institutions are facing with new issues relating to information security and computer networks invasion. Network (system) managers and ordinary users in an organization are all human factors that wrong motion of each one could have negative consequences associated with information security So, development projects has begun in response to the increased possibility of criminal activities and also to provide stringent security measures in communications and processing(Alhogail, 2015). However, if we have the best hardware or operating systems but our users or human factors don't do anything regarding security so we won't be successful. In this regard, this study plans to review the safety of users on using information technology and explain the role of each available component.

2. Information Technology

IT is a set of tools, techniques and methods of production, processing, storage and dissemination of information (Azadi Ahmadabadi, 2009). Mansell considers the following potentials and capabilities for Information Technology. Data creation: new innovations in information technology square away high speed networks to provide the possibility of creating and managing large amounts of information tailored to the needs of users and development goals. Providing production opportunities: information technology provides and increases many opportunities for producers. Scientific and technical knowledge sharing Support: the usage of information technology plays an important role in scientific and technological research, and finally the changes in the economic and social norms; so the communication speed increases the speed of decision-making (Mansell, 1999).

This technology stepped in the field of scientific and industrial fields two decades ago; and today, it is considered as an interdisciplinary expertise in the integration of computer science, informatics, mathematics, telecommunications and knowledge management technologies on the list of world new technologies (Rahmani, 2009). The most important feature of information technology is that their technological capabilities increase and the cost of their usage decreases continuously. At present, investment in this sector is increasing significantly.

3. Security of Information Technology

In the past half-century the world has seen many changes. The personal computer revolution in the mid-70s caused computers with supersize and strength to be available for hundreds of millions of people. In addition, Internet and other types of private networks have made the relationship between the panties very easy and common. Unlike 25 years ago, which working with computer and communication were done only by a few experts in this field, today hundreds of millions of computers are used for process of any imaginable information by users who are mostly amateur or non-professional and are linked together by a powerful social network named Internet. Obviously, with the development of technology, problems getting bigger and along with the development of science and technology, ways of taking advantage of it is grown too (Sadowsky and et al., 2003).

Development in the field of communications is due to human stunning achievement in the field of computer science and hardware and software and knowledge of IT and telecommunication. New communication and satellite communication equipment and Internet have diminished geographical

boundaries and have submitted new human communication and culture to human population. However, these advances in science and technology have provided great facilities yet have caused new problems to human population. However, this technology has caused facilitate communication and wide development, but have provided a space for abuse of offenders to disrupt human by abusing information, destruction of information and making living or working space unsafe. Network hackers follow different goals which different aspects of human life like political, economic, security and social aspects are subject to hackers (Ayati, Mohammadzadeh., 2007).

Speed factor in IT and communication is something about microseconds which caused invisible information to the naked eye controlled by software and developed by individuals could be moved or replaced. In this environment, illegal and destructive actions occur so rapidly it will be difficult to identify. Developing countries should also consider security as a top priority because the risk of further criminal activities is focus on the places where doesn't have sufficient control and are unsafe (Sadowsky and et al., 2003).

4. Importance of Study

Optimum use of information and its harmony and availability is one of the most important needs to achieve organizations to the goals that ultimately will follow increase in efficiency of organizations. In this regard, Storing information electronically, organizations have to use computers widely, computer channels especially internet. But it is clear that many dangers threatening computer systems, information, activities and its depend critical infrastructures and abuse in cyber space is different from real space so that saboteurs of cyber space consider their behavior as a crime without victims an honor and neglect the damage caused by it integration of that is one of the most important needs of organizations to achieve organizational (Colwill, 2010).

With the advancement of civilization and the formation of communities and security range found wide dimensions and with the separation of the field of property and personal rights of each other and public property and definition of national territory gradually included wide definitions such as privacy, social security, financial, political, national and economic security. In recent decades, especially in the past five years, the world has witnessed significant developments in many of the previous equation has changed substantially. According to many experts, similar to the effect of line and write the destiny of man, into the virtual space of modern information and communication technologies in a new era of human civilization has made (Shafiee, 2014).

But this big change accordingly requires applying numerous actions that one of their most important one is new concepts of security. Due to the growth of small local networks to wide and global networks, the need to protection and electronic security systems to guarantee exchanges and create a legal obligation has found more importance. Yet, security is growing but technology and security actions on soft wares and hard wares are not enough and sometimes individuals in organizations can make great damage considering that insiders usually have legal and significant access to facilities and information, organization knowledge, its processes and valuable properties location, security of human resources within the organization is important. Some significant internal threats are as follows: (Colwill, 2010)

- 52% of organizations do not have a formal assessment about security risks.
- 67% of organizations do not any control to prevent leaving of confidential information.
- 84% of companies do not investigate leaving confidential information via outgoing email.

It should be noted that many of the problems caused by people within the organization comes more from ignorance of the destructive impulses and unexpected failures that happened, the probability of large, interrelated effects of large-scale increase. Although absolute security is unattainable but a good level of security will attract trust and ensure of natural and legal individuals, companies and organizations to establish information and exchanges. This concept is really important especially for small and large

organizations in developing countries (Sadowsky and et al., 2003) and is more crucial than ever which address it.

5. Background of research

Today, several studies have been conducted regarding IT and user's safety which can mention to the one titled "Human Security and the application of new information technologies and communication" presented at International Conference on human security in West Asia in December 2008 by Ayati & Mohammadzadeh. Also, the paper titled "The Role of Human Error in Successful Security Attacks", by Fran Howarth which presented in Security in Intelligent in September 2014 is one of the leading studies of abroad in this field.

6. Objectives of Research

The following are some of the objectives of the present study that are worth mentioning:

- Evaluating the role of human factors in implementing or compromising information technology (IT) security.
- Planning for future improvement of security for real or legal (organizational) users.
- Raising awareness among ordinary and professional users as well as organizational personnel and managers.

7. Hypotheses

The main hypothesis: there is a significant relationship between components of information technology (IT) and users' information security.

Sub-hypotheses:

1. There is a significant relationship between users' concern with security of personal computer (PC) and their information protection.
2. There is a significant relationship between users' necessary attention to E-mails and their information security.
3. There is a significant relationship between users' necessary attention to choosing appropriate passwords and their information security.
4. The administrative staff takes antivirus installation and constant update seriously, and organization pays proper attention to purchasing and installation of original copies of antivirus software.
5. The conditions of information protection, implementation of access levels, and signing of security protocols agreement in the organization are not at the desired levels.

8. Methodology

In this research, the data has been collected by the Information Technology questionnaire. It is consisted of 36 multiple-choice items (questions) and 4 essay questions designed in 5 parts. The entered values are 0 if the response to a question is negative and 1 if the response is affirmative. There are several methods for reliability assessment such as test-retest method, rational equivalence and split-half method or Spearman's correlation coefficient and Cronbach's Alpha [De Vaus, 2002]. Using Cronbach's Alpha, the reliability of the questionnaire has been measured to be 0.74; its validity has also been confirmed by experts of the matter. The value of 0.74 for Cronbach's Alpha indicates that the questionnaire is desirably reliable. The questionnaire has been designed so that by reaching conclusions based on participants' responses, more accurate findings about security and its importance for IT users can be obtained. It is obvious that the results obtained from this questionnaire can help IT experts achieve a more complete idea of security and a better understanding of users' needs, and improve the ideas and concepts of

information technology among its different users. This questionnaire has been randomly distributed among 60 employees of Abhar County ministry of education working in different sections and departments such as public relations, information and communication technology unit, financial affairs, and planning and management development department; the questionnaires have been collected after being filled out.

9. Data Analysis

As mentioned earlier, the statistical population of the present study is consisted of employees of Abhar County ministry of education, among whom 60 individuals have been randomly selected as members of the sample group. Based on the information obtained from 54 collected questionnaires, the demographical features and characteristics of members of the sample group are as follows. Table 1 demonstrates the demographical characteristics of the sample group in terms of age:

Table1: The demographic characteristics of age in studied sample

Age	Number
≤ 30	34
< 40 < x30	9
≥ 40	8
Unknown	3

As demonstrated in the table, 56.6 percent of the employees are under 30, 15 percent are between 30 and 40, and 13.3 are over 40 years old; also 3 individuals have not mentioned their age in the questionnaires.
Table 2 demonstrates the demographical characteristics of the sample group in terms of employment record and experience of working with computers, based on the information obtained from 54 collected questionnaires:

Table 2: The demographic characteristics of work experience in computer field in studied sample

Work experience	Number
≤ 5	14
< 10 < x 5	30
≥ 10	5
Unknown	5

As the table show, 23.3% of employees had 5 years' work experience, 50% of them had experience between 6 and 10 years, 8.33 per cent over 10 years and the same amount of them were unclear.
Table 3 shows demographic characteristics of the level of education from collecting data of 54 questionnaires:

Table 3: The demographic characteristics of the level of education in computer field in studied sample

Education	Number
associate degree	12
bachelor degree	35

Master degree	5
PhD	2

As the data suggests, 20% of employees had an associate degree, 58.33 percent had bachelor degree, and 8.33 percent had MSc and 2 people holder PhD degree. The introduction of variables and data analysis option discussed as follow (Abundance of positive responses are given in appendix)

a) Personal Computers

Computer security is a branch of technology known as information security and information systems of any unauthorized access, use, disclosure, disruption, modification or destruction of physical and logical aspects. Security of personal computers usually is divided into two aspects of physical security and software. Physical security includes issues such as theft, bad weather, accidents and other risks are physical while security software can include broader aspects of the most important of which include phishing attacks, hackers, software crime, and pointed out DOS attacks. But the physical security of the workplace and equipment and the tools available to it are something which unnoticed by a lot of institutions. Despite the existence of such programs is compiled of great importance, its formulation by taking into account all factors and possible conditions is not so easy. As to protect the information on a computer against software attack many methods are used, it is important to ensure the physical security of the information against theft, loss or destruction must provide measures thought, so some of the most important elements of physical protection of personal computers can be outlined as follows (Noori, 2014).

- Maintenance of computer systems against unauthorized
- Check the security of the location of the system in the presence or absence
- Using video surveillance or alarm motion at work or home, if possible
- Use a safety locking cable

In this part four questions were asked for assessment of the personal computer factor and pursuit of its objectives and notifying users' attitude toward valuation of protecting their PC. Except the first three questions which have got specified answer (yes or no) and values of 0 or 1 for each import, the final question that has 4 options for backing up data intervals. Table 4 shows the frequency of these responses:

Table 4: The questions and results regarding the evaluation of employees' concern with PC security

	Question	**Negative responses (%)**	**Positive responses (%)**
1	Have you chosen any passwords for your display screen?	31.5	68.5
2	Do other people around you know your password?	88.9	11.1
3	Do you log-off your computer when temporarily leaving your work desk?	46.3	53.7
4	Do you regularly make back-up copies of your information?	35.2	64.8

As the obtained results show, in the first question, 31.5 and 68.5 percent gave negative and positive answer respectively which can say that setting password for log on to desktop is really important for majority of people and it is good to be considered by others. Also, second question has 88.9 percent negative response and 11.1% positive response which positive answers show the majority of people care about the confidentiality of their password. Third question with 53.7 percent positive response indicates

that more than half of people lock the screen when they temporary takeoff from their desktop. Fourth question showed 35.2 percent negative and 64.8 percent positive response which indicates that about one-third of people do not make backup of their data and it's better to pay more attention to this issue so by giving more information, it can be a culture in the organization.

b) Email

Many years ago, when there was no e-mail and computer so communication systems were paper based, people were afraid of revealing content of their letters. The loss of honor and dignity of the individual, political, social and cultural reasons to think it will provide secure communications systems. With the advancement of science and enter the field of computers, a new strategy for the exchange of information and correspondence provided human. Mail system is much faster than doing a paper. But like the traditional system, there was a problem with security and also the security of the system was exchanged messages (Raja, 2011). In e-mail, there are several protocols and mechanisms and, of course, within this mechanism and there will be risks. Many companies have published web email client software that enables users via the web, read their mail. Very high and popular implementations such as Hotmail, Yahoo and Gmail that enables users via a web browser, connect to the mail server itself are not secure and should implement strategies to secure them (Courtis, 2006). In this section, as before, 4 questions relate to the user important in connection with electronic mail security measure. Table 5, questions and answers show great results.

Table 5: questions and results regarding the evaluation of employees' concern with E-mail security

	Question	Negative responses (%)	Positive responses (%)
1	Do you open any anonymous or unidentified emails?	64.8	35.2
2	Do you click on any web links in your emails?	68.5	31.5
3	Do you open any attachments in your emails?	75.9	24.1
4	Do you sign-out after finishing using your email on a shared computer or device?	18.5	81.5

As the data suggests, the first, second and third question faced 64.8, 68.5 and 75.9 percent negative response respectively, indicating that the majority of people don't like to open unknown e-mails, invalid links and attachments and 81.5 percent agreed to Sign Out their e-mail service after using. According to the policies of an organization's information regards security of their staff and also to increase these values, this issue should be notified more than before.

c) Password

One of the most common ways of maintaining security in the virtual world of electronic components is using passwords. Password combination of letters, numbers, symbols, or a combination of any of these options is that they have been specifically created for use by each of the various components used very simple password. Set of numbers from one to nine, full name, the name of the place, date of birth, mobile phone number and a lot of numbers and phrases such cases by this category of users is considered as the password in If this type of easily guessable passwords and malicious people using the software can be easily discovered passwords. But whatever it is possible to guess their passwords more complex, and the length is, the security services are used by more users, because the disclosure or theft of a password, other passwords and other security services difficult does not risk no. This section consists of 11 questions

relating to the security of a password to the user the importance of their passage measured. Table 6 shows the questions and abundant of results:

Table 6: questions and results regarding the evaluation of employees' concern with password security

	Question	Negative responses (%)	Positive responses (%)
1	Do your different passwords contain any common words or phrases?	35.2	64.8
2	On an average, are there enough characters in the passwords you choose? (based on the criteria explained in the questionnaire)	38.9	61.1
3	Is it possible that you have exposed your password to other people around you?	50	50
4	Do your passwords usually contain a combination of letters and numbers?	38.7	61.3
5	Do you use special characters (@ # $ % ...) when choosing your passwords?	38.9	61.1
6	Do you regularly change your passwords?	68.5	31.5
7	Is the interval between the times you change your password short enough? (based on the criteria explained in the questionnaire)	42.6	57.4
8	Do you use easy-to-guess words and numbers (ID card number, birthday date, or phone number) when choosing your password?	40.7	59.3
9	Do you write down your passwords somewhere? (notebook, mobile phone, or computer file)	79.5	20.5
10	When writing down your password, do you also encrypt it in order to prevent exposure?	85.2	14.8
11	Have you chosen "always remember" option so that you don't have to enter your password every time?	20.4	79.6

As the result shows, 64.8% of people use the same password in their various components. The second question asked the number of characters used as password, if the number is less than 8 characters, a value of 0 to 8 characters or more considered and if it has a value of 1 was entered. In this section 61.1 percent have been recorded 8 or higher. On the third question, 50% of people inform other about their password which is high ratio. The next question, 3.61 of employees use a combination of letters and numbers for their password, and the rest use only letters or only numbers for it. 61.1 percent positive response, according to the fifth question, more than half of them use special characters. 31.5% of subjects in the sixth question change their password periodically and that the low level of the number of positive responses, 57.4%, the monthly period considered for the job. 59.3 and 20.5 respectively eighth and ninth questions percentage of favorable responses indicate that more than half of the respondents to guess their passwords, a fifth of it in a place where notes and of these, 14.8 of the time of writing, are encrypted. Question eleventh with 20.4 percent negative, set their password in the "always keep" form. With these results, it seems that the security situation in the use of passwords is not an ideal situation and the need to improve it to enhance the security of individuals and organizations, the more effort.

In general, high-security encryption that the following principles in its creation are observed:

1. be long: The longer a password is, the harder it will be to break and more time will be needed.

2. Be Unique: The unique name of famous people, cities and countries name, name and many other well-known words in the dictionaries of words, the worst option for a password is unique so it is best meaningless words elected as a password.
3. combination: a symbolic break that consists only of one word is much easier to break coded word addition, a number and a symbol also used it and used it in both large and small letters are mixed; But Unfortunately, compliance with these principles is not possible for all users who comply with the principles of a long-established password and remembering long passwords is difficult and it will be more difficult when the number of such codes to be increased.

d) Antivirus

When the enemy is equipped with new tools and methods to create a new deception, it is natural that the other side should also be equipped with new tools have to be overcome. This law applies to cyberspace as well. In the first half of the 1980s and viruses were often highly controlled laboratory researchers and thus they couldn't find a way to the outside world. But in early 1986, the first personal computer virus or as self-replication software was called Brain, was discovered. The virus would spread through 5.25 inch Floppy disks. However, compared with the viruses of today did very poorly, but the point of entry of the virus to the outside world and the beginning of the emergence of viruses, worms and malware that we today buckle. Today, with the growing development of technology and as a result, technology, manufacturing and distribution of malicious files and annoying, many anti-virus no longer old and, in fact, an anti-virus alone cannot be held accountable, and this is one reason New versions of security software are trying to provide users with a variety of capabilities and preventive measures. Three questions for this section are intended to assess this important characteristic of information technology in organizations paid. Table 7 shows the results of this assessment questions and abundance.

Table 7: The questions and results regarding the evaluation of employees' concern with antivirus security

	Question	Negative responses (%)	Positive responses (%)
1	Do you care about the antivirus program being always installed on your device?	5.6	94.4
2	If the answer to the previous question is yes, do you regularly update your antivirus program?	18.5	81.5
3	Have you purchased the original copy of the antivirus software installed on your device?	79.6	20.4

As the table depicts, 49.4% of them permanently installed an anti-virus on their systems. Of those positive answers, 81.5 percent are constantly updating them. Also the answers to the third showed that 79.6% of employees didn't purchase original one and suggest buying such useful program due to benefits of this software, so it is good that the organizations allocate special more budget over it.

e) Organization

Edgar Henry Schein had believed corporate culture as a set of beliefs and shared values and public perceptions, which was maintained by the organization. Products and innovations is the first level that includes all phenomena that one can see, hear and feel and doing things like language and processes. The visible surface is (what it is). The second level is the support values, including values about how things

should be done (what should be) and the third level or below the level of the underlying assumptions is that the feelings, values and personal accounts of employees of an organization should act is (what could be). This level is not visible in people's minds. According to the three levels of Edgar, culture is defined as "organizational culture is a set of basic assumptions of the organization in the face of problems, to adapt to the environment and achieve internal unity, created as a result of this culture as the correct way to perceive, think and feel transported to new members.

This concept argues that by adding a fourth layer with the knowledge and expertise of employees in connection with the three-layer security provided by Edgar Schein organization, can a culture of information security in the organization. It also tries to show that demand for security management and employee participation seriously, with mutual respect. In an ideal culture of information security, each of the four layers should be stronger than the minimum acceptable level of harmonization and alignment as well. Because of importance of this issue, 14 questions have been allocated to this. Table 8 shows the results of this assessment questions and their abundance:

Table 8: questions and results regarding the evaluation of employees' concern with organization's information security

	Question	**Negative responses (%)**	**Positive responses (%)**
1	Is the antivirus program you use at work the original copy purchased by your organization?	51.9	48.1
2	Does the organization practically values implementation of security on its IT systems (by providing security software, hardware, and etc.)?	46.3	53.7
3	Is the budget the organization spends on security enough?	38.9	61.1
4	Are you and your co-workers adequately concerned with observation of security protocols in the organization?	13	87
5	Are there any educational or training programs regarding IT security in your organization?	42.6	57.4
6	Do the organizational users ever sign a legally binding document regarding observation of security protocols?	75.9	24.1
7	Does the organization implement any reward/punishment system for observation/breaking of security protocols?	68.5	31.5
8	Do only authorized users have the access to computer systems in the organization?	77.8	22.2
9	Are there any software/hardware security measures such as unique username and passwords for authorized users?	31.5	68.5
10	Are authorized users allowed to view/use other network users' information?	66.7	33.3
11	Are there any policies implemented for limiting password expiration time in the network?	42.6	57.4
12	Are the authorized users in different departments required to change their passwords regularly?	66.7	33.3
13	Are the original and back-up copies of software/information safely maintained?	31.5	68.5
14	Do you give away your own password to your co-workers or allow them to use your personal work space?	83.3	16.7

This gathered information showed that the 48.1% of employees have purchased the original version of anti-virus and 53.7 percent stated that the organization's security concept and its application is value for them.In the next two questions which allocate 0 to poor choices and 1 for medium and higher choices, 61.1 percent of people have evaluated the importance of the security and 0.87 percent had positive view to the importance of respondent and his colleagues. 57.4 percent said that they implemented training programs in this which are not favorable and the organization should pay more attention to this. Also, 75.9 percent of those in the sixth question of law the observance of security commitments signed by the employee in an organization do not exist. In question number seven, 68.5 percent of employees have reported the lack of incentive and disciplinary actions against compliance or non-compliance of security agencies in organization. However, in 8th question it was found that only 22.2 percent was agreed that only authorized users have access to computers which this amount is very small. Of these result, 68.5 percent believed that there is hardware and software to limit the use of others. Also, in question 10, 33.3% stated that authorized users can access to each other's information.

10. Theoretical analysis of the essay questions

Among 54 answered questionnaires, 22 (41 percent) contain valid and acceptable responses in the essay questions section. The criteria for validating and acceptance of the responses are explained in the following sections. Concerning the first question regarding "the role of organization in establishment of regular back-up, computer lock, and other matters which usually are not considered to be important" most of the responses point out the importance of developing the culture and necessary trainings by the organization. Holding training sessions, emphasizing the importance of security in computers and computer networks, carrying out security tasks by a server, setting a timer and software on the systems, monitoring of the systems and information entry and extraction by informatics departments in organizations and institutions, security regulations, and development of punishments and rewards for observation of security protocols, raising awareness about the pros and cons of valuing security, sending memos on security and putting reminders beside computers, and regulations for creating back-up copies are among solutions proposed in the answers regarding security culture among private and organizational users. Considering the current culture of the society, one of the participants believes that important issues should become "mandatory" in order to be taken seriously.

Concerning the second essay question regarding e-mails, the participants point out issues such as refraining from opening anonymous or advertisement emails, subscribing personal emails in insecure websites, opening emails which could contain spam content, or using antivirus to detect possible malwares in emails, deleting spam mails without opening, use of antivirus programs which are able to evaluate security of the website links, use of firewalls, refraining from activities which may expose email addresses, implementation infrastructures that can filter unsuitable materials, raising awareness, educating, and introducing antivirus programs to prevent threats and damages caused by emails. However some participants are not optimistic about the effectiveness of any methods to be used in this regard. Concerning the third question regarding passwords, the participants make suggestions such as use of letters and numbers and characters altogether, not saving passwords on other computers, refraining from choosing familiar and easy-to-guess passwords, choosing complex passwords, refraining from choosing passwords which are used for other purposes such as ATM or mobile phone or safe password, choosing a password with at least 8 characters, regular change of password, refusing to give away the password to others, refraining from writing down the password, or encrypting the written password if need be. The fourth and last essay question deals with organizational users' weakness in implementation of security. The responses indicate that organizations have little commitment to information protection. Most of the computers are used publicly and without any access authorization. Due to the use of free operating systems and high price of antivirus programs, the software programs are not original and the antivirus programs are not regularly updated. The managers are not particularly keen on expending in this field.

Individual users are usually accounted for updating the antivirus programs, and they usually do not carry out this task seriously. Organizational users' awareness is low. Failing to understand digital security concepts, as well as users' reluctance toward security issues and exposing their passwords to others due to inaccessibility of organizational information in different user levels are other problems which have been mentioned.

In the end, considering these interpretations and regarding the normality of the data, Pearson's parametric test can be used in order to analyze the data. The results of Pearson's test of correlation between dimensions of IT and user security are demonstrated in table 9.

Table 9: results of Pearson's test of correlation between dimensions of IT and user security

Variables	correlation coefficient	Significance level
PC	0.39	0.01
Email	0.44	0.01
Password	0.58	0.01
Antivirus	0.43	0.01
Organization	0.21	0.01

As we know, the null hypothesis in correlation test indicates lack of correlation. Here, since Sig=0 <0.05, therefor the null hypothesis is rejected. This means that the hypothesis i.e. the existence of correlation is confirmed. On this sense, based on Pearson's correlation coefficient and significance level reported in table 9, there is a positive and significant relationship between dimensions of IT security and users' security. The strongest relationship belongs to "password security". Also table 10 demonstrates the results of multiple regression analysis of dimensions of IT and user security.

Table 10: the results of multiple regression analysis of dimensions of IT and user security

Variables	The coefficient of determination	The Adjusted Coefficient of Determination	Significant level
Components of Information Technology in Department of Education	0.389	0.376	0.01

The results presented in table 10 indicate that the adjusted coefficient of determination for linear relation of dimensions of IT security and users' security equals 0.376. This means that components and dimensions of IT explain 37 percent of the variance in user security variable.

11. Conclusion

Nowadays, digitalized methods of storing organizational information and documents and increased volume of information on one hand, and rapid and growing threats before this information on the other have made security a crucial and vital issue.

Considering the obtained information, the first hypothesis regarding the significant relationship between users' attention to PC security and information protection is confirmed. Also the results suggest that there

is a significant relationship between necessary attention to emails and users' IT security as well as between optimal choice of password and users' IT security; there for the second and third hypotheses are also confirmed. Considering the high percentage of positive answers regarding administrative staff's concern with installation and constant updating of antivirus program, the fourth hypothesis is confirmed; however, concerning the second part i.e. organization pays proper attention to purchasing and installation of original versions of antivirus software, the results obtained from 54 questionnaires prove otherwise. In the end, the results confirm the fifth hypothesis i.e. conditions of information protection and implementation of access levels and security protocols and regulations in the organization are not at the desired levels.

Also, regarding the answers to the essay questions, the participants' responses to the existing problems are manifested as solutions such as increasing individual's responsibility and accountability, informing and raising awareness, development of culture, regulating of the security issue, establishment of informatics department in organizations for consistent monitoring of individuals and computers, information update carried out by a certain accountable individual or department, distribution of educational materials and CDs among employees by the organization, and keeping personal passwords confidential and secret by the employees. The present study suggests that despite the efforts in recent years, the extent to which employees and authorities take information protection seriously is far less than ideal. Mere finance of required security measures such as purchasing original copies of antivirus programs by individuals or organizations is not going to be enough. More time and money should be spent in order to overcome the existing defects in this organization and other similar organizations. It should be noted that aside from damages sustained by organizational data, many personal users have been victimized because of improper attention to security issues. Authorities should proceed with regulating and legislating security measures and holding employees responsible in order to meet the standards of this sensitive matter. Considering the speed and strength of malwares, users and authorities should spend more on learning these subjects. Suggestions made in this research as well as other books, articles, and educational media are waiting to be applied by users and authorities. The researchers sincerely hope that in the near future these concepts are established and threats are averted so that human resource and financial costs are reduced and organizational productivity is improved.

References:

Ayati, Mohsen; Zadeh, A., 2007, "Human security and the use of new information technologies and communication", International Conference on Human Security in West Asia

Alhogail, Areej. (2015). Design and validation of information security culture framework. Computers in Human Behavior. Vol. 49. 567–575.

Azadi Ahmadabadi, Gh. and A., 2009, IT in KM, applications and effects, comprehensive portal. Human science design.

Colwill, Carl. (2010). "Human factors in information security: The insider threat- Who can you trust these days?. Information security", technical report.

Curtis Smith, 2006, "Pro Open Source Mail: Building an Enterprise Mail Solution",apress Sep 26.

De Vaus, D. (2002). Surveys in Social Research (5th ed.). London: Routledge. Ch.

Hoonakker, Peter, Bornoe, Nis, Carayon, Pascale. (2009). "Password Authentication from a Human Factors Perspective: Results of a Survey among End-Users". Center for Quality and Productivity Improvement. ISyE Department, University of Wisconsin-Madison, USA, IT University, Copenhagen, Denmark, Proceedings of the HUMAN FACTORS and ERGONOMICS SOCIETY, 53rd Annual Meeting.

Motameifar, M., 2008, "Implementation of data security standard (ISO 27001) in organizations (including checklists applicable)", first edition, Tehran, broadcast center and Industrial Research of Iran

Noori, B., 2014, “security of personal computer ", Pars Data website, Tehran

Mansell, R. 1999, “Information and communication technologies for development: assessing the potential and the risks”, Telecommunications Policy, 23, 35-37.

Raja, SH; 2011, "security of e-mail", published by Pendar PARS, Tehran, Iran

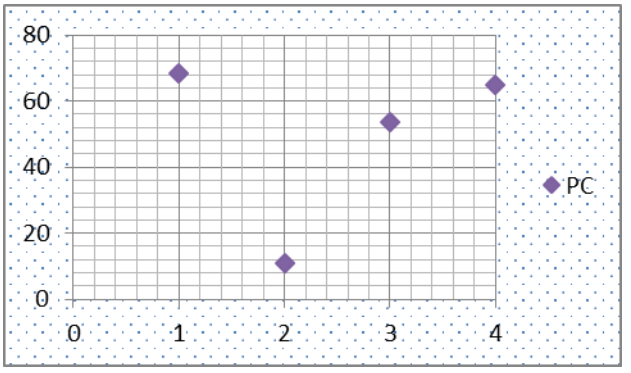
Rahmani, S. 2009, Evaluating the effect of information technology on knowledge management, master's thesis, University of Allameh Tabatabai.

Shafiee, Sanaz. (2014). Studying the Effective Factors on Domestic Tourists Trust in Offering EServices in E-Tourism: Case tudy Iran Country. 8th International Conference on e-Commerce. 24 - 25 April 2014, Mashhad, Iran.

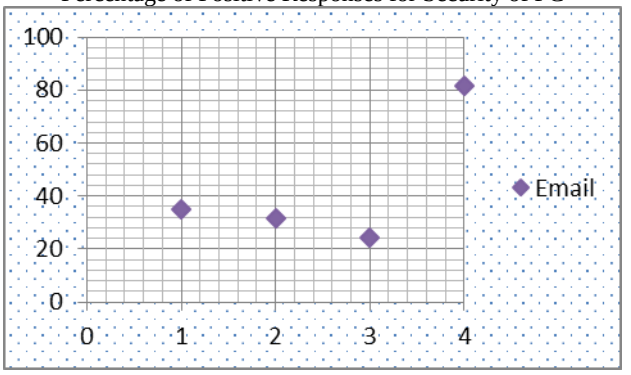
Sadowsky ,George; James X. Dempsey; Alan Greenberg; Barbara J. Mack; Alan Schwartz; 2003,” IT Security Handbook”; infoDev, Worldbank.

Taghipour, Mohammad, Mahboobi, Maryam; Yaghoubi, Jafar, 2014, "A Study of IT applications in knowledge management, public high schools Alborz Province", the first international conference on knowledge management, Shahid Beheshti University.

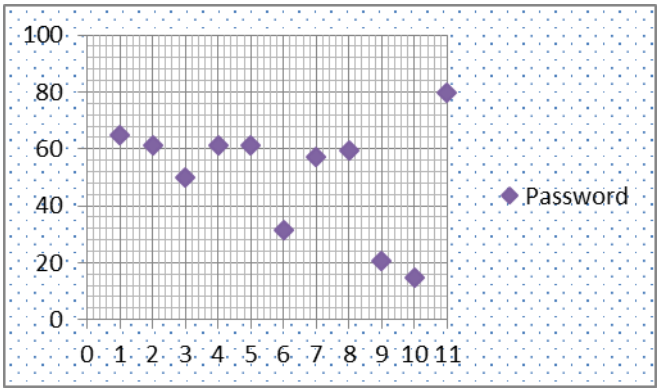
Appendix



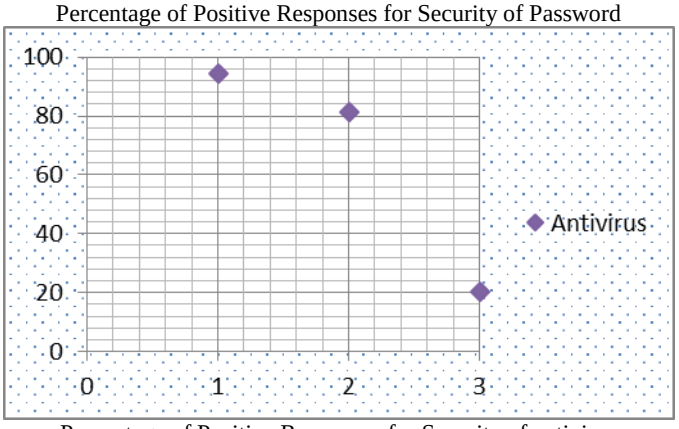
Percentage of Positive Responses for Security of PC



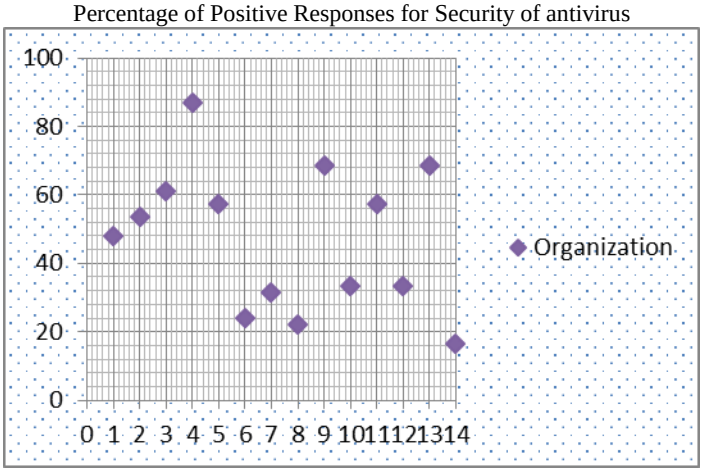
Percentage of Positive Responses for Security of Email



Percentage of Positive Responses for Security of Password



Percentage of Positive Responses for Security of antivirus



Percentage of Positive Responses for Security of The organization