Ethical Hacking in the Saudi Government Institutions

Shaymaa Mousa, Wejdan Barashi
Business and Administration Faculty, King Abdulaziz University
shaymaarashad@yahoo.com

Abstract

The Internet has become indispensable to governments by allowing them to conduct E-government, provide better citizen service, improve communications, and access needed information rapidly. While computer networks have revolutionized the way governmental institutions operate, the risks they introduce via interconnectivity can be devastating. Attacks on computer systems via the Internet can lead to lost money, time, reputation, and sensitive information. One reaction to this state of affairs is a behaviour termed "Ethical Hacking" which attempts to proactively increase security protection by indenturing and patching known security vulnerabilities on systems owned by other parties. The main purpose of this study is to address the problems related to the ethical hacking in governmental institutions in Saudi Arabia. The results show that there is a lack of awareness to issues of information security, and ethical hacking, Ethical hacking have a positive impact on the Saudi institutions, and most of ethical hacking problems in Saudi Arabia are related to senior management, staff, society and laws. More researches are needed to consider other measures and include other countries which may show different results.

Keywords: Information security, Ethical hacking, Computer Ethics

1. Introduction

In the age of globalization, people are more dependent on high technology such as the internet and information systems as part of their daily lives. In the realm of government, high technology is promising to enhance the delivery of public goods and services to citizens by using e-government. Although the explosive growth of using high technology in governmental institutes has carried many valuable things: increasing the efficiency of the process and management of government. On the other hand, it raises up some drawbacks concerning the ethics. Most of organizations face several cybercrimes such as criminal hackers. With these concerns and others, the ethical hacker can help. Although ethical hacking is one of today's necessities in the fight against cybercrimes, many people misunderstand what ethical hacking is. Many of the pirating and web corporations became famous such as Anonymous, Wikileaks, and OpIsrael. According to a report from the Al- Arabia Website in November 2009, Saudi Arabia is defined as the most vulnerable Gulf States to attacks of hacking and piracy. It recorded 796,000 cases of malfunctions of computer systems which represents 64% of the total number of cases in the Gulf Cooperation Council [1]. In May 2013, Al- Arabia website have recorded the hacks of several Saudi Ministries and governmental sites, and posted the pictures on their Twitter accounts [9]. According to these statistics, the need to apply ethical hacking in governmental institutions, universities, organizations become a security important requirement. Due to the importance of this subject, a number of researches focus on the study of ethical hacking. Their studies focus on issues like lack of understanding, non-clarification of laws regarding ethical hacker, and non-enforcement of information security standards in various organizations. The aim of this paper is to measure awareness extent of Information security and determine the impact of the ethical hacking on governmental institutions in Saudi Arabia. Survey methodology is used as a base for this research. The rest of this paper is organized as follows:

Section 2 describes ethical hacking. Section 3 illuminates literature review. Section 4 shows methodology. Section 5 is results and discussion. It end with conclusion in Section 6.

2. Ethical Hacking

Ethical hacking is an assessment to test and check an information technology environment for possible weak links and vulnerabilities. Ethical hacking describes the process of hacking a network in an ethical way, therefore with good intention [2]. Ethical hacking plays an important role in evaluating the information security of organizations by giving a pointer for organizations to weaknesses in their systems to prevent security breaches. By this way, ethical hacking increases the empowerment of information security of these organizations and enables them fighting E-terrorism and supporting the national security [5, 8]. There are two groups of ethical hackers: White-hat hackers and black-hat hackers. White-hat hackers are those who are usually security professionals with a knowledge of hacking and the hacker toolset. They use their knowledge to trace weaknesses. It is critical for them to get permission prior to beginning any hacking activity [3]. In contrast, the black-hat hackers use their skills and abilities to invade the privacy or intellectual property of others, breach systems, or destroy them. They use the same methods and techniques of White-hat hackers. They frequently do that out of political, social, religious, or cultural reasons.

An ethical hacker's evaluation of a system's security seeks answers to three basic questions: 1) What can an intruder see on the target systems? 2) What can an intruder do with that information? 3) Does anyone at the target notice the intruder's attempts or successes? [2].

3. Literature Review

Prior research has identified several important issues regarding ethical hacking. This prior focus on issues like lack of understanding what is the hacking and its types, non-clarification of laws regarding ethical hacker, and non-enforcement of information security standards in various organizations.

[2] Describe what ethical hacking is, what it can do, an ethical hacking methodology as well as some tools which can be used for an ethical hack. They suggest that an ethical hackers do not need to hide his traces as he is testing the client environment comprehensively.

[6] Show that ethical hacking is nothing new. It has been an accepted term in the world of information security for quite some time. They mention that ethical hacking provide a unique solution to secure the client networks. Furthermore, they indicate that no security plan guarantee success, and without management support, failure is guaranteed. [6] Figure out after organizations have identified risks, enlisted services, and digested the results of ethical hacking activities, remediation efforts must be planned and engaged. They find out that maintaining security is dynamic and flexible process.

[4] Try to differentiate between a criminal hacker and an ethical hacker. They demonstrate how the ethical hack strengthen the security of the overall systems environment. They notice that there is so much confusion surrounding what makes hacking ethical and unethical and its subsequent legal treatment.

[5]Investigate the method of how to help keep ethical hacking, ethical. Also, they discusses how much can we trust ethical hackers? They explain the idea of teaching people how to hack systems becomes ethical issue and on the ethical considerations for teaching ethical hacking. They identify that none can ever be certain of the intentions of someone else, so the blame cannot reside with the teacher. Moreover, they indicate that none can prove if it is ethical to teach people how to bypass these physical security measures because their skills are necessary when used ethically. They suggest using different models to monitor employees closely to reduce the risk of impact. It can also decrease the impact by identifying implications early enough to help reduce the impact of confrontation.

[10] Aim to report the profile and the individual opinions of the students of Alexander Technological Institute in fundamental ethical and social principles. They show that the students faced some issues when it comes to ethics and social responsibility, this was due to: students lacked the critical thinking skills, which helps them

to make better choices. They recommend that a separate course in Ethics would substantially raise the chances of more ethical awareness amongst the IT students.

4. Methodology

This study aims at assessing the study samples awareness extent of Information security, illustrate the concept of ethical hacking knowledge, shows the impact of the ethical hacking, also, list the problems of ethical hacking from the study sample point of view.

Four educational organizations were included in the study: King Abdul Aziz University, King Saud University, King Fahd University of Petroleum and Minerals, and King Abdullah University of Science and Technology. Five non-educational organizations were included in the study: Jeddah Municipality, Riyadh Municipality, Saudi Arabia Airlines, the Ministry of Communications and Information Technology, Communications and Information Technology organization. These organizations represent the most important organizations in different regions in Saudi Arabia: Central Region, Western Region and Eastern Region. Researchers wanted to distribute the questionnaires in Saudi ARAMCO, which considered one of the most important organizations in the Kingdom of Saudi Arabia based in the Eastern region to become there is convergence between the numbers of organizations according to the zone. The IT manager had been addressing, who showed his willingness but the rejection came from the Department of Public Relations of the organization do not allow the distribution of questionnaires in Saudi ARAMCO.

A random sample of 303managers and employees from information technology and information security departments was gathered, 226 for non-educational sector and 75 for educational sector. The determining Sample Size from a Given Population table was used to determine the size of the sample to be withdrawn from the target community [7].

The survey questions aimed to know the targeted samples' perspective and their view regarding the systems used in their companies. A survey questionnaire consists of three basic parts as follows: Part I, which aims to gather demographic information on the respondents such as name, specialization, position, and years of experience. Part II aims to collect general information about ethical hacking in the organization. Part III aims to achieve the objectives of the study and answer its questions. this part contains four dimensions which comprise 43 items that will be measured using a five-point Likert scale, where (1) strongly disagree, (2) disagree, (3) Not sure, (4)agree, (5)strongly agree. (See Appendix 1 for more details).

Participated organizations categorized as educational sector and non-educational sector. Educational sector includes King Abdul Aziz University, King Saud University, King Fahd University of Petroleum and Minerals, and King Abdullah University of Science and technology. Non-education sector includes Municipality of Jeddah, Municipality of Riyadh, Saudi Arabian Airlines, Ministry of Communications and Information Technology, and Communications and Information Technology organization.

Test of questionnaire study stability was conducted by Alpha Cronbach's lab for each axis of the Study axes.

5. Results And Discussion

The survey results analyzed using the statistical program SPSS version11.The 303 questionnaires gathered from sample. Two samples excluded because the answers are not completed. As a result, the total number of sample become 301.

The result of first part of the questionnaire clarify that (33.6%) of education sector respondents in contrast, (82.7%) of non-education sector are specialized. According to years of experience, the percentage of who have five years or less of experience is came (48.7%) for education sector in contrast, (32%) non-educational sector.

The second part of the questionnaire, clarifies that the percentages of respondents in the both sectors, who have agreed of the existence a specialized section for information security, is (75.2%) and (90.7%)

respectively of the total respondents and this is important for all organizations. The respondents in the educational and non-educational sectors are not sure of the existence of a ethical hacking in the organization by (60.6%) and (50.7%) respectively. In the educational sector, (54.5%) of respondents who answered 'yes', confirm that ethical hacker outside the organization, while non- educational sector percentage is (3.33%.). The majority of his answers were not sure that the organization is performing hacking testing that in educational and non-educational sectors with percentages (67.7%) and (56 %) respectively.

The following is the third part which shows the sample answers to the following four axes: information security, the concept of ethical hacking, its impact and its problems.

Information Security

Table[1] shows the sample responses about information security phrases axis in the educational & non-educational sector.

	Educational		Non-educational	
Degree staff feedback	Repetition	Percentage%	Repetition	Percentage%
Strongly Disagree	12	5.2	–	–
Disagree	39	17.3	3	4.0
Not sure	58	25.7	20	26.7
Agree	82	36.3	41	54.7
Strongly agree	35	15.5	11	14.6
Total	226	100.0 ٪	75	100.0 ٪

Table 1: The responses about information security in the educational & non-educational sector

From table 1, it is clear that the proportions of respondents who have sufficient information security in the education sector and non-educational (51.8%) and (60.3%), which is low for the staff of information technology and information security in organizations.

Concept Of Ethical Hacking

Table [2] shows the sample responses about concept of ethical hacking phrases axis in the educational & non-educational sector.

	Educational		Non-educational	
Degree staff feedback	Repetition	Percentage %	Repetition	Percentage%
Strongly Disagree	2	0.9	–	–
Disagree	13	5.8	3	4.0
Not sure	105	46.5	25	33.3
Agree	96	42.4	45	60.0
Strongly agree	10	4.4	2	2.7
Total	226	100.0 ٪	75	100.0 ٪

Table 2: The responses about ethical hacking in the educational & non-educational sector

Table 2 shows that educational and non-educational respondents answered towards the concept of ethical hacking awareness is (46.8%), and (62.7%).Whilst (46.5%) and (33.3%) not sure.

Table 1 and 2 show that a proportion of specialists in both sectors do not have the awareness and knowledge of the existence of a specialized section for information security and the ethical hacking.

The organization has a defect in the conduct of tests, or it does not educate or alert the staff and users when doing these tests. Lack of awareness among managers and staff of the issues of information security and ethical hacking and conduct of tests, therefore there is a great lack of awareness in society in general. The lack of awareness of ethical hacking is due to the novelty of its conception and not discussed in studies and researches in the Arab world, particularly in Saudi Arabia, and that the organizations may deliberately hide dealing with this technique in information security.

Effect Of The Ethical Hacking

Table[3] shows the sample responses about effect of the ethical hacking Phrases axis in the educational & non-educational sector, terms that E1, E2, ... explain numbering of questionnaire phrases.

	Educational			Non educational		
Phrases	The weighted average	Weight percentile%	Order	The weighted average	Weight percentile%	Order
E1	3.79	69.75	2	4.20	80.00	1
E2	3.76	69.00	3	3.87	71.67	3
E3	3.61	65.25	4	3.76	69.00	4
E4	3.57	64.25	5	3.76	69.00	5
E5	3.86	71.50	1	4.17	79.33	2
E6	2.97	49.25	7	3.32	58.00	6
E7	3.10	52.50	6	3.05	51.33	7
E8	2.96	49.00	8	2.81	45.33	8

Table 3: The responses about effect of the ethical hacking in the educational& non-educational sector

The above table 3, shows that clarifies the effect of ethical hacking in the educational & non-educational sectors that were ranked as the mentioned in the table. The educational and non-educational sectors agreed that the rankedE1 and E5 phrases are the most influential. It is considered the most important positive effects on the organization.

Ethical hacking has a positive impact on organizations, the most important impacts are: Ethical hacking makes employees more aware in dealing with information security issues. Ethical hacking is considered one of the most important techniques used to ensure the security of the organization. Ethical hacking increases the credibility of the organization. Ethical hacking enhances the commitment to the client. Ethical hacking increases the competitive advantage to the organization.

Problems Of Ethical Hacking

Table[4] shows the sample responses about problems of the ethical hacking Phrases axis in the educational & non-educational sector, terms that P1, P2, ... explain numbering of questionnaire phrases.

	Educational			Non educational		
Phrases	weighted average	Weight percentile%	Order	weighted average	Weight percentile%	Order
P1	3.45	61.25	2	3.33	58.25	1
P2	3.16	54.00	6	3.04	51.00	5
P3	3.49	62.25	1	3.33	58.25	2
P4	3.40	60.00	4	2.84	46.00	6
P5	3.38	59.50	5	3.17	54.25	4
P6	3.42	60.50	3	3.27	56.75	3

Table 4: The responses about problems of the ethical hacking in the educational& non-educational sector

The above table 4, shows clarifies the ethical hacking problems in the educational & non-educational sectors that were ordered as the mentioned in the table.
Educational and non-educational sector agreed on that the most important ethical hacking problems affecting organizations in Saudi Arabia are the phrases No. P1, P3, and P6, respectively. While respondents of non-educational sector phases No.2,4 are not considered a problem of ethical hacking in organizations. This applies with practice, where the possibilities of non-educational sectors outweigh the educational sectors.
Concludes from the above, the most important problems of ethical hacking in the educational and non-educational sector in Saudi Arabia are those relating to senior management, staff, society and laws.

6. Conclusion

Governments, companies, and private citizens around the world are apprehensive to be a part of this revolution, but they are afraid that some hacker will break into their Web server and replace their logo with pornography, read their e-mail, steal their credit card number from an on-line shopping site, or implant software that will secretly transmit their organization's secrets to the open Internet.
This study aims to discuss the ethical hacking and its issues and influence on information security in governmental entities in Saudi Arabia. Nowadays, Saudi governments have become more dependent on the information systems. The benefits of the development of this system enormous, including access to high-efficiency organizations, improve communication with customers, services, and the quality. Also, it increases the competitiveness of countries power.
The result of this study shows the lack of awareness for managers and officials of information security. Also, it finds that ethical hacking has a positive influence on the organizations, as the sample individuals picked from the organizations have agreed on two impacts; it makes managers and officials more aware of information security issues, and that it's one of the most important techniques used to ensure the security of the organization. In addition, it figures out that one of the main problems of ethical hacking within educational and non-educational organizations are related to the lack of senior management, staff, and society awareness.
This study confirms that in both educational and non- educational sectors, there is a lack of information security awareness among employee. Also, the years of experience in the sectors are less than five years for most of employees.

It's noticeable that the education sectors hire security specialist's more than administrative cadres in information technology. Moreover, that clears that non –educational sector already have information security specialists. This explains why government educational sectors are typically dealing with competent foreign

companies and organizations for testing their system using ethical hacking. And as for a non- educational governmental sector that provides services or products, they depend on staff from within the organization. There is lack of awareness of managers and staff to issues of information security, ethical hacking and performance tests.

The educational and non-educational sectors response agreed that phrases as follow: ethical hacking one of the most important techniques used to ensure the organization information security and applying ethical hacking in the organization makes employees more aware to deal with information security issues, are the most important positive effects on the organization.

Educational and non-educational sector agreed on that the most important ethical hacking problems affecting organizations in Saudi Arabia are these phrases respectively, Problems related to senior management, Problems related to staff, laws, and society. While respondents of non-educational sector a Problems relating to the capabilities of the organization, and Problems relating to implementation, are not considered a problem of ethical hacking in organizations. This applies with practice, where the possibilities of non-educational sectors outweigh the educational sectors.

The percentage of respondents in the educational and non-educational sectors in general is not sure with their big percentage in most phrases; this confirms what has already been mentioned, a lack of awareness among managers and staff information technology and security departments in the organizations in the information security issues.

7. References

[1]Ajbaili,M. *Saudi & UAE at high risk to cyber-crime*: report, al-arabiya news,dubai,(2009).Available:http://www.alarabiya.net/articles/2009/11/15/91411.html

[2] Baumann,R.*Ethical hacking*,(2002), Accessed:February15,2012.Available:http://www.giac.org/registration/gsec

[3] Graves, K. CEH® *Certified Ethical Hacker StudyGuide*,Indianapolis: sybox& wily, (2010).

[4] Jain, B, Ravi,K.*Hacking- Ethical or Criminal-A Legal Quandary*,The Icfai University Press, (2008).

[5] JAMIL,D andALI KHAN,M.*Is Ethical Hacking Ethical*,International Journal of Engineering Science and Technology(IJEST), Vol .3 No.5. (2011),pp. 3758-3763.

[6] Kraus,R.ISSA member,*Ethical hacking from start to success*, ISSA Journal,San antonio,USA, (2009),pp.14-18.

[7] Krejcie,R and Morgan,D. *Determining Sample Size For Research Activities*, In Educational And Psychological Measurement. University of Minnesota,Texas A. & M. University, (1970) , pp.607-610.

[8]Pondent, C. eHow Contributor *The Advantages of Ethical Hacking* Accessed:May7,2012. Available:http://www.ehow.com/info_8431442_advantages ethical-hacking.html

[9] Reuters. *Saudi Arabia says hackers sabotagegovernment websites*,Al-arabiya news,Riyadh,KSA,(2013)Available:http://english.alarabiya.net/en/media/2013/05/18/Saudi-Arabia-says-hackers-sabotage-government-websites.html

[10] Voutsa, A.E , Siakas,V. E , Nisioti ,S. K , and Ross, M, *Survey of Informatics Students' Awareness on Ethical Issues*, The British Computer Society , (ISBN 1-902505-77-8). (2006), pp. 139-150.

APPENDIXES

Appendix1

- **First part :**

1. (Name) optional .....

2. Specialization

○Computer Science ○Computer Engineering
○Information Security ○Information Systems
Other○

3. Position

○IT Manager ○Employee in IT department
○IS Manager ○Employee in IS department
○ Ethical hacker ○ other

4. Experience years

○ Less than five ○ 5 - 10
○ 11 - 20 ○ More than 20

- **Second part :**

1. Does the organization have information security department?

○ Yes ○ no

2. Does the organization have an ethical hacker?

○ Yes ○ no ○ Not sure

3. If the answer to the previous question is (yes), are ethical hacker from inside or outside the organization?

○ Inside the organization ○ outside the organization

4. Does your organization perform hacking testing?

○ Once a year ○ More than once a year
○ None ○ Not sure

- **Third Part :**

Statement	Strongly Agree	Agree	Not sure	Disagree	Strongly Disagree
Information security					
You have enough knowledge about information security					
You have a full knowledge about the legislation and the laws regarding to information security					
There are big threats to the governmental organizations in security information					
Security procedures in the organization are sufficient to ensure information security					
The organization has clear policies for information security					
Concept of ethical hacking					
You have sufficient knowledge about the meaning of ethical hacking					
There is a difference between the ethical hacking and unethical hacking					
Monitoring the employees activities by their managers via his PC's considered ethical hacking					

One of the most important objectives of ethical hacking is detected system loopholes and promote level the organization security					
Ethical hacker does not fix the security weaknesses					
Ethical hacker has the rights to access all information in Organization					
Ethical hacker should contract with organization before starting his work					
Effect of the ethical hacking					
Ethical hacking one of the most important techniques used to ensure the organization information security					
Ethical hacking increases organization reliability					
Ethical hacking enhances the client obligation					
Ethical hacking increases the competitive advantage of the organization					
Applying ethical hacking in the organization makes employees more aware to deal with information security issues					
Your organization got (ISO) after applying ethical hacking					
Hacker can access unauthorized organization's resources					
Misuse of information by ethical hacker					
Problems of ethical hacking in your organization					
lack of IS senior management awareness about the importance of ethical hacking					
Information security officials are with poor experience regarding the ethical hacking legal and administrative procedures					
Ethical hacker doesn't have sufficient knowledge & experience					
The higher cost to hire professional ethical hackers in the organization					
Instructions and legal contracts between ethical hacker and organization are not clear					
Loss of confidence in the ethical hacker					
The system and services failure for a period of time					
Lack of specialists in ethical hacker					
The organization does not have management risk assessment					
Infrastructure that supports information technology in the organization is poor					
Current system is not updated continuously					
Size of the organization does not encourage the use ethical hacking					
The organization lacks the alternative plans to deal with the crisis					

Statement	Strongly Agree	Agree	Not sure	Disagree	Strongly Disagree
Information security					
You have enough knowledge about information security					
You have a full knowledge about the legislation and the laws regarding to information security					
There are big threats to the governmental organizations in security information					
Security procedures in the organization are sufficient to ensure information security					
The organization has clear policies for information security					
Concept of ethical hacking					
You have sufficient knowledge about the meaning of ethical hacking					
There is a difference between the ethical hacking and unethical hacking					
Monitoring the employees activities by their managers via his PC's considered ethical hacking					
One of the most important objectives of ethical hacking is detected system loopholes and promote level the organization security					
Ethical hacker does not fix the security weaknesses					
Ethical hacker has the rights to access all information in Organization					
Ethical hacker should contract with organization before starting his work					
Effect of the ethical hacking					
Ethical hacking one of the most important techniques used to ensure the organization information security					
Ethical hacking increases organization reliability					
Ethical hacking enhances the client obligation					
Ethical hacking increases the competitive advantage of the organization					
Applying ethical hacking in the organization makes employees more aware to deal with information security issues					
Your organization got (ISO) after applying ethical hacking					
Hacker can access unauthorized organization's resources					
Misuse of information by ethical hacker					
The slowness handling of the crisis					
No information backup to be used in case of crisis					
Previous crisis management programs are not evaluated to improve them for future					

Statement	Strongly Agree	Agree	Not sure	Disagree	Strongly Disagree
Information security					
You have enough knowledge about information security					
You have a full knowledge about the legislation and the laws regarding to information security					
There are big threats to the governmental organizations in security information					
Security procedures in the organization are sufficient to ensure information security					
The organization has clear policies for information security					
Concept of ethical hacking					
You have sufficient knowledge about the meaning of ethical hacking					
There is a difference between the ethical hacking and unethical hacking					
Monitoring the employees activities by their managers via his PC's considered ethical hacking					
One of the most important objectives of ethical hacking is detected system loopholes and promote level the organization security					
Ethical hacker does not fix the security weaknesses					
Ethical hacker has the rights to access all information in Organization					
Ethical hacker should contract with organization before starting his work					
Effect of the ethical hacking					
Ethical hacking one of the most important techniques used to ensure the organization information security					
Ethical hacking increases organization reliability					
Ethical hacking enhances the client obligation					
Ethical hacking increases the competitive advantage of the organization					
Applying ethical hacking in the organization makes employees more aware to deal with information security issues					
Your organization got (ISO) after applying ethical hacking					
Hacker can access unauthorized organization's resources					
Misuse of information by ethical hacker					
Low use of original software and licensed					
Organization ethical values is not documented					
The organization does not encourage employees to devise new security solutions					

Statement	Strongly Agree	Agree	Not sure	Disagree	Strongly Disagree
Information security					
You have enough knowledge about information security					
You have a full knowledge about the legislation and the laws regarding to information security					
There are big threats to the governmental organizations in security information					
Security procedures in the organization are sufficient to ensure information security					
The organization has clear policies for information security					
Concept of ethical hacking					
You have sufficient knowledge about the meaning of ethical hacking					
There is a difference between the ethical hacking and unethical hacking					
Monitoring the employees activities by their managers via his PC's considered ethical hacking					
One of the most important objectives of ethical hacking is detected system loopholes and promote level the organization security					
Ethical hacker does not fix the security weaknesses					
Ethical hacker has the rights to access all information in Organization					
Ethical hacker should contract with organization before starting his work					
Effect of the ethical hacking					
Ethical hacking one of the most important techniques used to ensure the organization information security					
Ethical hacking increases organization reliability					
Ethical hacking enhances the client obligation					
Ethical hacking increases the competitive advantage of the organization					
Applying ethical hacking in the organization makes employees more aware to deal with information security issues					
Your organization got (ISO) after applying ethical hacking					
Hacker can access unauthorized organization's resources					
Misuse of information by ethical hacker					
The organization Staff don't have enough information about social engineering					
The staff do not accept accessing their personal information by ethical hacker					

Statement	Strongly Agree	Agree	Not sure	Disagree	Strongly Disagree
Information security					
You have enough knowledge about information security					
You have a full knowledge about the legislation and the laws regarding to information security					
There are big threats to the governmental organizations in security information					
Security procedures in the organization are sufficient to ensure information security					
The organization has clear policies for information security					
Concept of ethical hacking					
You have sufficient knowledge about the meaning of ethical hacking					
There is a difference between the ethical hacking and unethical hacking					
Monitoring the employees activities by their managers via his PC's considered ethical hacking					
One of the most important objectives of ethical hacking is detected system loopholes and promote level the organization security					
Ethical hacker does not fix the security weaknesses					
Ethical hacker has the rights to access all information in Organization					
Ethical hacker should contract with organization before starting his work					
Effect of the ethical hacking					
Ethical hacking one of the most important techniques used to ensure the organization information security					
Ethical hacking increases organization reliability					
Ethical hacking enhances the client obligation					
Ethical hacking increases the competitive advantage of the organization					
Applying ethical hacking in the organization makes employees more aware to deal with information security issues					
Your organization got (ISO) after applying ethical hacking					
Hacker can access unauthorized organization's resources					
Misuse of information by ethical hacker					
There are no procedures for authorizing computer room access					
There is no specified procedure about using information system after official work hours					