Journal of Computer Science 2 (3): 229-235, 2006
ISSN 1549-3636

An Empirical Study of Attitudes and Opinions of Computer Crimes: A Comparative Study between U.K. and the Kingdom of Bahrain

Adel Ismail Al-Alawi and Mohamed Fathi Abdelgadir
Department of Management Information Systems, College of Information Technology
University of Bahrain, P.O. Box 32038, Kingdom of Bahrain

Abstract: In this digital age we are constantly becoming more reliant on technology and information systems in all walks of life. There is no doubt that Computer systems play a fundamental role in the basic operation of almost all organizations today. The emergence of the Internet has played a major role in exploiting new opportunities and markets for many businesses today and has also revolutionized the way information is shared globally. With the increased use of computer networks as a means of sharing data, the need to protect and preserve the integrity of data arises due to the increase in unauthorized access of organizational computer systems. It has become a major challenge for organizations to identify and counter these threats. Computer crime has emerged as one of the major forms of sabotage causing millions of dollars worth of damage annually. These attacks usually come in the form of viruses, worms, denial of service attacks and hacking this study will attempt to compare the opinions on computer crimes of the online society in the Kingdom of Bahrain with that of a study conducted in Great Britain. Similarly this study will also try to measure the perceived level of safety the online public enjoys and use these results to determine weather there is a relationship between the perceived level of online safety and the willingness to conduct online transactions. The issue of "software piracy" will also be discussed with respect to copyright laws in the Kingdom of Bahrain.

Key words: Computer crime, copyright, software piracy, UK, Bahrain, attitude

INTRODUCTION

Before discussing computer crime it is important to understand that computer crime does not always refer to crimes that take place using the World Wide Web as a medium or gaining unauthorized access to a computer system. Computer crime is a very general term describing crimes that take place using a computer or crimes that are directed towards a computer system.

The research will focus on computer crimes such as the creation and spread of viruses, denial of service attacks, sabotage and unauthorized access to computer systems. This study will also try to determine public awareness and opinions on these types of crimes. Since opinions may differ from one individual to another. Another factor that will be measured is the perceived level of safety enjoyed online or in other words "how safe people feel when they are online" this factor will provide the basis to either support or disapprove the following hypothesis:

H1: The perceived level of safety is a factor in the willingness of the public to conduct online transactions.

Literature review: Computer crime is defined as "A violation of law committed with the aid of, or directly involving, a data processing system or network"[1]. As Norton and Stockman[2] illustrated in their study, the whole point of a network is to connect computers to each other. A computer in a locked room without any connections is almost perfectly secure, but once it is connected to another computer or device, it becomes vulnerable. This statement indicates that computer crime would not be possible if a computer were locked in a room and deprived of network access. It also implies that for computer crime to exist a computer would in some way need access to the outside world. The Internet or any other WAN, LAN or MAN usually facilitates this access; however, this does not apply for theft of computer equipment.

As Gilbert[3] stated "Today we live in a technologically driven era, with advances in communications and computing continually appearing. Along with the benefits of technological advances we also become exposed to antics of malicious and curious persons that want to penetrate our network, read our email, scan our databases, alter organizational records, infect our storage with viruses and perform other harmful acts."

According to Dowland *et al*.[4] whose research this study is based on "Highly publicized incidents of computer crime and abuse have significantly contributed to the Internets reputation for insecurity.

Corresponding Author: Adel Ismail Al-Alawi, Department of Management Information Systems, College of Information Technology, University of Bahrain, P.O. Box 32038, Kingdom of Bahrain, Mob: +973-36779000

As such, it is useful to determine more specifically how such incidents are perceived and the possible effects this may have". These incidents may have a negative effect on individuals who are active on the Internet. It may also contribute to people who are online regularly to feel unsafe.

The types of computer crime which are discussed in this study include:

Distributing viruses: Malicious code which may infect data processing systems and cause them to slow down or even destroy sensitive data.

Viewing someone else's data: This includes opening another person's files without his/her prior consent.

Altering someone's data: This includes opening another person's personal files and altering them.

Theft of computer equipment: Taking organizational computer equipment without permission.

Unauthorized copy of software (software piracy): Copying protected software without the consent of the owner.

Unauthorized copying of data: Copying protected material without permission of the author.

Computer fraud: Using a computer to commit any type of fraud.

Sabotage: Using a computer to attack other systems for the purpose of disabling or destroying the system.

The views and opinions on the severity of various forms of computer crime may vary from one individual to another. Some individuals may view some types of computer crime such as the illegal copy of software as something very minor; others may not find it to be a crime at all. Opinions may vary widely on this subject, which is why this study aims at evaluating the opinions of the online society in the Kingdom of Bahrain. The second part aims at evaluating the safety factor, which involves measuring how safe people feel decimating information online. This was tested by finding peoples opinions on giving out information online, purchasing products online etc. Furthermore, the results of the attitudes on computer crime will be compared to a study conducted by Dowland *et al*., which investigated the opinions on the computer crimes discussed above in the United Kingdom. A major purpose of the study was to observe the differences and similarities in opinions between the two countries.

"Destruction or alteration of data" was ranked the most significant type of computer crime by respondents in a survey conducted by the American bar associations task force on computer crime[5]. This may be because financial damage is caused when IS professional spend a lot of time scanning records to maintain data integrity[6].

The Internet has also created a portal for hackers to destroy data[6]. Because of the increased use of web sites by organizations to offer their services, hackers attempt to deface websites by altering the content or leaving a mark which is the equivalent of street graffiti where someone adds offensive text or images to a website. This usually affects an organization's business in a negative manner because customers who realize that the site has been breached may never return. This may be similar to a consumers view on a bank that has been robbed; the customer would most probably not want to put his money in this bank because of the security risk.

Web pages are not always altered for the purposed of vandalism. Groups of individual may have other motives for altering the information on a web site. Other reasons may be political or religious. Because web sites can be a very effective form of spreading the word terrorists may target frequently visited website to spread their message. To counter this these organizations need to constantly monitor their web sites to ensure the authenticity of their web pages[7].

Another major menace comes in the form of computer viruses, which act in the same manner as biological viruses. Biological viruses attack living tissue while destroying cells and multiplying afterwards. In the same way computer viruses are usually hidden in legitimate programs and attack computer systems by penetrating these programs and sending themselves to other computer systems usually via email. Apart from destroying files, viruses can slow down communications because they cause programs to process huge number of messages and data for no particular purpose, which greatly reduces the efficiency in sending legitimate messages. The word "Virus" and worm are usually used interchangeably although "worm" usually refers to a virus, which is spread through networks[8].

All of the above-discussed computer crimes may affect the level of safety an individual enjoys while online. This study will try to determine the views of the Bahraini society on the above computer crimes. This study will also attempt to measure the perceived level of safety enjoyed by the online society in the Kingdom of Bahrain. Further elaboration on the issue of "software piracy" with respect to Bahrain's copyright laws is discussed as follows:

Copyright laws in the Kingdom of Bahrain: Copyright laws were introduced in the Kingdom of Bahrain in 1993. According to law decree No. 10 for the year 1993 in respect of the protection of copyrights. The Law was enforced on June 9, 1993. The law included the following statement for computer programs: "The protection period for computer

software shall expire after fifty years have elapsed from the date of completion of the work, or after forty years have elapsed from the date of publication, whichever is nearer[9].

Software piracy in the Kingdom of Bahrain: The piracy situation has somewhat improved over the years following the Ministry and Cabinet Affairs and Information's (MOI) 1998 enforcement campaign. Although copyright laws were introduced in 1993 in Bahrain the enforcement campaign did not begin until 1998. Under this campaign retailers were given until Feb. 28, 1998 to legalize their trade in videos, CDS and computer programs. The MOI conducted many raids and even closed down shops that violated the law. These efforts however have only been effective in combating video piracy. The business software industry still remained a problem with hard disk loading and end user piracy still remaining. It is very common in Bahrain for individuals to exchange software, which is unlicensed. The problem occurs because pirated software still enters the country; mainly from East Asian countries where software piracy is still a major problem.

As a member of the WTO (World Trade Organization) Bahrain was encouraged to bring its laws and enforcement campaigns into compliance with the agreement on Trade Related Aspects of Intellectual Property rights (TRIPS) by Jan 1st 2000. At this time Bahrain's copyright laws fell short of TRIPS compliance, as there were many gaps to be filled in enforcement.

To encourage a more effective enforcement campaign Bahrain was placed on IIPA'S watch list with an early out of cycle review to determine if Bahrain's further efforts merit removal from the watch list[10].

According to this study the copying of software was not considered to be a serious crime with only 24% considering it as a very serious issue. Because of the attitudes of the general public in the Kingdom of Bahrain it becomes very difficult to enforce these laws. If people don't consider software piracy to be a crime they will always tend to find ways to obtain illegal copies of software. The very best the MOI can do is to crack down on retailers to limit the access people have to illegal software. Another problem is neighboring Saudi Arabia where pirated software is still widely available. A lot of this software is brought into Bahrain and distributed cheaply. Recently, the Business Software Alliance, the group that represents Microsoft, Adobe and other software makers concerned about piracy, signed up another unusual partner -- the grand muftis at Al Azhar in Cairo. The highest religious authority in Sunni Islam, Sheikh Ibrahim Atta Allah, issued a fatwa, or edict, against piracy. "Piracy is the worst type of theft and is prohibited by Islam," Atta Allah declared. Despite this software piracy still remains a major problem in the Arab world[11]. At times people need a specific program to carry out a certain task. They would not consider buying the program because the software will only be used for a short period. A person would not think twice before loading his/her computer with an illegal copy of the program, simply because it is cheap and convenient and is not considered to be a crime or morally incorrect by the individual. Many people consider this as a way to save money and feel that corporations are ripping them off of their hard earned money.

Some efforts have been taken by the Bahraini government to combat software piracy by introducing a joint incentive between Microsoft and the Bahraini government in which government employees could obtain original copies of certain Microsoft software for a very cheap price. This technique aims at providing software for the individual at a very small cost; although, businesses would still have to purchase the software at full cost. Even though this method might prove effective, what will stop one individual for obtaining a copy of a program and distributing it freely to his colleagues and friends? This is one of the main reasons why fighting software piracy at the individual level is a very tedious task. If the end-user could be educated on the benefits of obtaining a legal copy of the software and at a cheap price, it might be a positive step towards eradicating software piracy to a certain degree. In this way the end-user would know the benefits of using a legal copy and would not need to obtain a pirated copy. Some benefits of legal copies include support from the vendor and updates for the software from the vendor. Table 1 shows the estimated trade losses for the Kingdom of Bahrain due to computer software piracy from 1998-2001.

Although the level seems to be decreasing over the years, it still is very high compared to other developed countries. Trade losses to the U.S. software industry were estimated at $2.3 million for 1998. Unfortunately despite the software industries repeated requests for specific information about enforcement actions, the Bahraini government has yet to provide full confirmation or details[12].

More recently Bahrain signed the Free trade agreement with the United States in 2004. This agreement reflects the Kingdom of Bahrain's commitment in combating software piracy and other forms of piracy. Excerpts of the agreement state that:

* Each government commits to protect copyrighted works, including phonograms, for extended terms (e.g., life of the author plus seventy years), consistent with U.S. standards and international trends.
* Each government commits to using only legitimate computer software, thus setting a positive example for private users.

Table 1: Trade losses from software piracy in the Kingdom of Bahrain (Adopted from IIPA)

Industry	2001		2000		1999		1998	
	Loss	Level	Loss	Level	Loss	Level	Loss	Level
Computer Programs: Business Application	2.3	87%	2.7	89%	4.2	92%	2.8	92%
Computer Programs: Entertainment Software	3.2	93%	3.1	95%	3.1	91%	3.4	94%

As mentioned earlier this requirement will be very difficult to enforce at the end-user level. This will require a tremendous effort in educating the general public to bring about a change in attitudes[12].

MATERIALS AND METHODS

The research uses a quantitative approach in which questionnaires were designed and distributed to different business sectors in the Kingdom of Bahrain. This is used to describe the incidence, frequency and distribution of certain characteristic of a population.

This research is specifically a descriptive quantitative research which is "an approach that involves either identifying the characteristic of an observed, pre-existing phenomenon or exploring possible correlation among two or more phenomena"[13]. This approach aimed at solving the first problem, which was to determine the awareness and opinions on computer crime in the Kingdom of Bahrain. The first part of the questionnaire was related to demographic details. The second part of the questionnaire was designed to test the individuals Internet habits to obtain a general idea of his/her exposure to the Internet. Another section of the questionnaire was designed to test the opinions on the safety of using the Internet and finally the last section was used to test the awareness of computer crime in the Kingdom of Bahrain.

The questionnaires: In order to ensure an appropriate conceptual framework to work within two channels were used to distribute the questionnaire. The first channel was the traditional paper-pencil, which were distributed to students, employees and faculty members of various universities in the kingdom of Bahrain. Similarly, they were also distributed to managers and employees of prominent businesses such as Gulf Air, Aluminum Bahrain and Bahrain Telecommunications Company. The second channel used was the online questionnaire. The questionnaires yielded approximately 500 responses in total, although some questionnaires were discarded because of incomplete information. Statistical tests were conducted using the SPSS statistical software package, which is specialized software that facilitates the analysis of any research findings. The statistical tests included tabulation, independent sample t-test and ANOVA.

RESULTS

The survey demographics showed a female dominance in all age groups, with 55% of the total respondents being female as compared to 80 % males in the UK Study. Most of the respondents were below the age of 30, with 85% of the respondents falling in this group. The results also showed that 46% of the respondents were from the Information Technology field while 33% were from the Business field. The breakdown of the respondent age groups is shown in Table 2.

Table 2: Age distributions of respondents

Age		Valid Percent	Cumulative Percent
Valid	77.3	77.3	77.3
	8.0	8.0	85.2
	5.7	5.7	90.9
	2.8	2.8	93.8
	4.5	4.5	98.3
	1.7	1.7	100.0
	100.0	100.0	

In terms of education 65% of the respondents had at least a degree level of education as compared to 44% in the UK study. Over 50% of the respondents claimed to have used the Internet everyday while the rest either used it once a week, few times a week or few times a month. The respondents spent an average of 12 hours per week on the Internet. When asked what they spent the most time doing online 32% answered, "general surfing" while only 3% answered "shopping".

From the above information it is safe to say that a large majority of the respondents are active on the Internet and that they are suitably qualified to comment on the issues covered in this study. Table 3 shows the descriptive for gender.

Table 3: Gender descriptive

Gender	Frequency	Percent	Valid Percent	Cumulative Percent
Female	97	55.1	55.1	55.1
Males	79	44.9	44.9	100.0
Total	176	100.0	100.0	

Opinions on computer crime and abuse: Generally over 60% of the respondents felt that computer crime and abuse was a problem as compared to 80% in the UK Study. A more detailed evaluation of the opinions on computer crime and abuse yielded the results shown in Table 4. The results shown in Table 5 were taken from the U.K. study.

Table 4: Views on computer crime and abuse in the Kingdom of Bahrain

	V. Serious %	Serious %	Not Sure %	N. Serious %	No Crime %
Viruses	70	19	5	3	3
Viewing someone else's data	41	40	7	9	3
Altering someone else's data	44	28	19	5	4
Theft of computer equipment	43	28	14	11	4
Unauthorised copying of software	24	32	18	15	11
Unauthorised copying of data	24	30	23	14	9
Computer fraud	35	26	26	9	4
Sabotage	30	20	39	6	5

Table 5: Views on computer crime and abuse in the United Kingdom Adapted from Dowland *et al*.[4]

	V. Serious %	Serious %	Not Sure %	N. Serious %	No Crime %
Viruses	71	17	9	1	2
Viewing someone else's data	29	37	25	4	5
Altering someone else's data	80	15	3	0	2
Theft of computer equipment	82	15	3	0	0
Unauthorised copying of software	18	22	36	13	11
Unauthorised copying of data	24	35	26	6	9
Computer fraud	70	20	9	0	1
Sabotage	90	6	3	0	1

Observations

1. Most of the computer crimes were considered to be of a serious nature by the respondents in both studies as shown in Table 4 and Table 5. This is observed by adding the serious and v. serious columns for each table. It illustrates that most of the respondents fell in the serious or very serious group for most of the crimes.
2. In the UK study theft of computer equipment was the only factor considered to be entirely criminal while in the Bahrain study none of the factors were considered to be entirely criminal.
3. In the UK study the incidents that had a clear analogy in the real world such as (theft, sabotage and fraud) were identified as being either 'serious' or 'very serious' with the majority of respondents falling in this area. This was not true for the Bahrain study. In the Bahrain study 71% of the respondents identified theft as either 'serious' or 'very serious', for fraud it was 61% and for sabotage it was a surprising 50% only. Some concern lied in the possibility of many of the respondents either not having a clear idea of the meaning of "sabotage" or completely misunderstanding the term.
4. Another interesting observation showed that 56% of the respondents in the Kingdom of Bahrain considered 'unauthorized copying of software' to be a serious issue while only 40% thought so in the UK. The copyright act was introduced in Bahrain in 1993. Until the year 2000 software piracy was very common and widespread in the Kingdom of Bahrain. It was not till late 2001 when the Ministry of Information began a nation wide crack down on software piracy by slapping heavy fines on any violators. Apart from this, the level of software piracy still remains high. It was expected that the percentage of respondents for this crime would be much lower than that of the UK because of the attitudes towards using illegal software in the Kingdom of Bahrain.
5. In both nations 11% thought that copying of software is not considered as a crime.
6 A relatively high number of respondents in the Kingdom of Bahrain replied to 'theft of computer equipment' as not being a crime. This result was unexpected. It was possible that some respondents confused this with borrowing computer equipment from the workplace although this is not likely as the question was very clear.

Safety analysis (determining level of safety): The safety analysis was used to determine the perceived level of safety enjoyed by the respondents. A series of questions that were related to giving out information over the Internet were used to determine where the respondent stood on this issue. The scores were then tabulated and used to determine the degree of safety enjoyed by the respondent. The results were then saved under a variable named 'safety.'

Skewness: The skewness produced by the safety analysis was 0.168. This indicates that there was a symmetrical distribution. This in turn indicates that the respondents enjoyed a medium or average level of safety. A Box and Whiskers Diagram was produced to provide more information on the distribution of the respondents.

Analysis of box and whiskers diagram: After tabulating the scores for safety and producing a Box and Whiskers Diagram from the results, the symmetrical area of the two boxes in the Box and Whiskers Diagram (Fig. 1) indicates that the mean for the perceived level of safety is very close to the mid-point. From the analysis the following results were obtained:

Lowest possible score:	4
Highest possible score:	20
Mid-Point:	12
Mean:	11
Median:	11
Skewness:	0.168

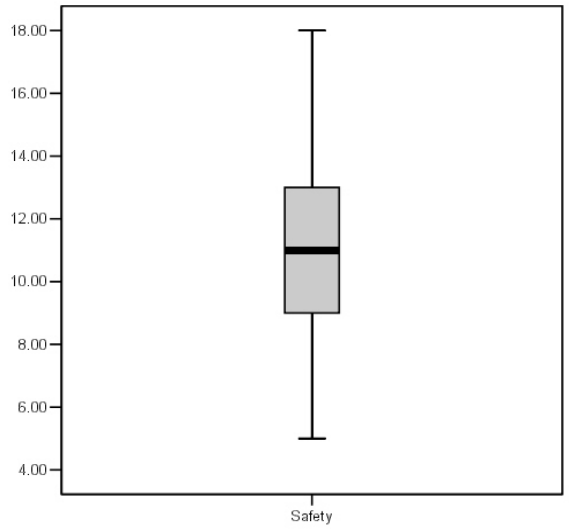

Fig. 1: Box and Whiskers diagram

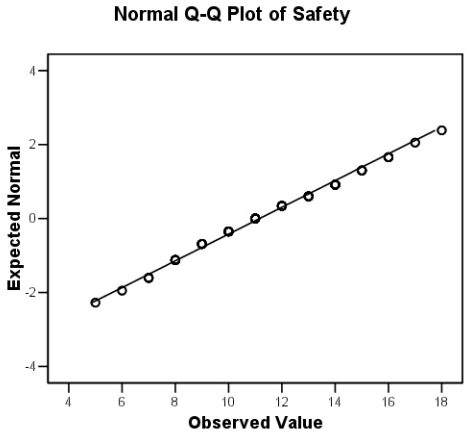

Fig. 2: Normal Q-Q plot

The mean is very close to the mid-point. From the value of the skewness, stem and leaf plot and the Box and Whiskers Diagram it is clear that the distribution of the safety scores is symmetrical which means the majority of the respondents enjoyed an average sense of safety. It was also observed that the number of respondents decreases as we move to the two extremes, which are a low and high level of safety.

The significance of this result becomes clear when we consider the two cases. Were the distribution to skew to the right, this would mean that the people were really panicking. If the distribution were to skew to the left this would mean that the respondents enjoyed a high level of safety or otherwise are indifferent to the parallels of the Internet.

To conclude the above analysis, it was observed from the results that the respondents enjoyed an average level of safety. In other words the respondents neither enjoyed a high level of safety while online nor did they feel very threatened.

The Normality of the scores was also checked by performing a Normal Q-Q Plot. All of the points on the diagram (Fig. 2) lie very close to the line. This indicates that the safety scores come from an approximately normal distribution.

Safety analysis (hypothesis): The last part of the research aimed at using the safety analysis results obtained above to give support to the hypothesis, which is mentioned in the beginning of the paper. After measuring the perceived level of safety the respondents enjoyed while online, the safety factor, which in this case represents the independent variable, was then used to determine if it affects the respondent's willingness to conduct certain transactions online.

ANALYSIS RESULTS

In the questionnaire the respondents were asked weather they would purchase products online. The respondents were asked about purchasing products online because it required the individual to give out personal information over the Internet such as full name, credit card no etc. in order to complete the transaction. In Table 6, the group, which indicated that they would buy products online, had a mean of (12.41) on the perceived safety online variable (SD= 2.75). On the other hand the group that indicated that they wouldn't purchase products online had a mean of (10.75) on the same variable (SD= 2.66). Table 7 shows the Levene's test for equality of variances. Table 8 shows that independent sample t-test indicated that the difference between the means of the two groups was significant at 0.001. The significance of the result means that the difference between the two groups can be generalized to the population from which the sample was drawn. This result also indicates that the groups willing to purchase products online are those who feel safer about giving out personal information online.

From the analysis results the conclusion was drawn that those individuals who felt safer (scored higher on perceived safety) while they were online had no problem with giving out personal information online. On the other hand those who did not feel safe online (lower score for perceived safety) did not feel comfortable giving out personal information online. The result of the analysis supports my hypothesis that "The perceived level of safety is a factor in the willingness of the public to conduct transactions online".

Group statistics

Table 6: Group statistics for safety

	Do you purchase products online	N	Mean	Std. Deviation	Std. Error Mean
Safety	Yes	41	12.4146	2.75659	.43051
	No	132	10.7576	2.66192	.23169

Table 7: Significance test

		Levene's test for equality of variances	
		F	Sig.
Safety	Equal variances assumed	.916	.340
	Equal variances not assumed		

Table 8: Significance test (continued)

t-test for Equality of Means						
t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% confidence interval of the difference	
					Lower	Upper
3.453	171	.001	1.65706	.47994	.70969	2.60443
3.389	64.865	.001	1.65706	.48889	.68063	2.63348

CONCLUSION

Computer crime and abuse will always be a negative aspect of Information Technology. As the use of Information Technology grows every day, new methods of using this technology for malicious activity will also grow. Despite the negative uses of technology the information society is always expanding at a constant rate as Information Technology has a positive effect in bringing the society closer together. There will always be individuals who will use technology negatively to satisfy their own personal greed or to harm others. Some of these motives may be personal while other may be professional. Some people may even commit some of these acts without being aware of the damage it causes to other individuals. It becomes necessary to educate the public on the negative effects these crimes have on individuals and society as a whole. If society start to lose faith in Information Technology it would be a major set back to the advancement of a nation. As Information Technologies were designed to make life easier for society, it would really be a waste if people were scared or felt unsafe while using these technologies. There will always be a risk no matter what you are doing, although these risks may be countered if society is educated on certain protective measures. This would be an important step in increasing societies faith in Information Technology and would contribute to increasing the overall quality of life.

REFERENCES

1. Alliance for Telecommunications and Industry Alliance. Computer Crime. http://www.atis.org/tg2k/_computer_crime.html. Accessed 5th December 2004.
2. Norton, P. and M. Stockman, 2000. Networking Security Fundamentals. (Ed.) Peter Norton's, United States, pp: 10, 27, 29.
3. Gilbert, 2001.
4. Dowland, F. et al., 1999. Computer crime and abuse: A survey of public attitudes and awareness. Computers and Security, 18: 715-726.
5. Power, R., 2002. CSI/FBI 2000 Computer Security Survey. Computer Security Institute.
6. Effy, Oz, 2002. Management Information Systems. 3rd Edn. Boston: Course Technology.
7. Ralph, S. and R. George, 2003. Principles of Information Systems. 6th Ed. Boston: Course.
8. Power, R., 2002. CSI/FBI 2000 Computer Security Survey. Computer Security Institute.
9 United Stated Trade Representative. Bahrain Free Trade Agreement. (ud) http://www.ustr.gov/document_library/fact_sheets/2004/Bahrain_Free_Trade_Agreement_Fact_sheet.html. Accessed 5th January 2004.
10. International Intellectual Property Alliance. Bahrain Copyright Laws. (ud) http://www.iipa.com.rbc/1999/rbc_bahraib_301_99.html. Accessed 2nd December 2004.
11. Susan, Postlewaite, 2002. A Fatwa on Piracy. http://www.law.com/jsp/statearchive.jsp?type=Article&oldid=ZZZ5YOJ9V1D. Accessed 4th December 2004.
12. International Intellectual Property Alliance. Bahrain Copyright Laws. (ud) http://www.iipa.com.rbc/1997/rbc_bahrain_301_97.html. Accessed 2nd December 2004.
13. Leedy, P.D. and J.E. Ormrod, 2001. Qualitative Research. Practical Research, (Ed.) Davis, K., Johnston, J.W., United States, pp: 147-159.