Cloud Computing and Data Science
https://ojs.wiserpub.com/index.php/CCDS/

UNIVERSAL WISER PUBLISHER

Research Article

Evaluating the Effect of Studying Computer Ethics and Computer Ethics Rules and Regulations on Computer Ethics at Work

Yas A. Alsultanny

Arab German Academy for Science and Technology, Germany
E-mail: alsultanny@hotmail.com

Received: 23 December 2019; **Revised:** 2 July 2020; **Accepted:** 2 July 2020

Abstract: With the increasing reliance on computer and Internet, the danger of cybercrime attacks was increased. This research paper aims to evaluate the effect of studying computer ethics and computer ethics rules and regulations on computer ethics at work. A self-administrated questionnaire was designed for data collection. The data was collected from 374 responds working in private and public sectors. The results showed a strong correlation between studying computer ethics and computer ethics rules and regulations, a strong correlation between studying computer ethics and computer ethics at work, and a moderate correlation between computer ethics rules and regulations and computer ethics at work. The gender and age have statistically significant effect on computer ethics at work, while education level and job position have no statistically significant effect on computer ethics at work. According to the respond's opinions, this paper recommends giving intensively interest in educating the computer ethics modules, to all levels of education as well as organizing continuous learning workshops to employees for all job positions, to increase awareness against computer crimes.

Keywords: internet, computer ethics, education level, cybercrime, computer crimes, continuous learning

1. Introduction

Internet has become an essential technology for communication, online conferencing, online teaching, and many others areas of applications. At the same time, increasing concerns about ethical issues created by the interconnecting world in the age of globalization. These concerns about privacy, misuse of computer resources, and even criminal activity abound are threatened all individuals, organizations, countries, and economies.

Computer ethics is rapidly developing and evolving into a wider and even more important field, thus it, reasonably, might be called "global information ethics" [1]. The Information and Communication Technology professionals were described the computer ethics concept through providing unethical computer using behavior. They considered computer ethics primarily as a component of Internet ethics [2]. Many of the news has focused on unethical accounting practices, thus the importance of computer ethics has also increased. In addition, issues such as Internet privacy, computer crime, intellectual property controversies, censorship, consumer trust, and other factors are at the forefront of business today [3]. Computer fraud cannot be prevented even with an improved risk control system and strengthening of computer security systems, this illustrates the need of good computer ethics and ethical behavior, the computer crime is a continuously

DOI: https://doi.org/10.37256/ccds.112020184

increasing problem across the world [4]. The traditional face to face learning ethics might not be applicable to online and distance learning environments due to the ethical issue fraud [5].

The computer ethics play a key role in all internet applications in preventing frauds. This paper was for evaluating the effect of studying computer ethics and computer ethics rules and regulations on computer ethics at work in the Kingdom of Bahrain. The next sections of this paper are organized as follows; the section outlines the motivations for this study, the section presents the research objectives, the section of related literature, the section of research model and methodology, the section of data analysis and discussion, and finally a section of the conclusion.

2. Motivations for this research

The motivations for this research emerge from the recommendations that appeared in the literature of the absence of cybercrime law in Bahrain and the disappearance of computer ethics from the university's curriculum, which increased the danger of computer crimes.

The Central Bank of Bahrain announced that some customer noticed a breakthrough to their bank accounts by rigging Automated Teller Machine (ATM) cards and credit cards, where the number of cards that were affected 174 cards [6]. In 2012, Interior Ministry's cybercrime unit in Bahrain recorded a total of 223 cases related to cybercrime, while in 2011 the number of cases recorded was 249.

Thus, it is certainly worthwhile to investigate the following significances in this paper;

1. Create awareness and help in reducing cybercrimes.
2. Increasing the level of computer ethics by pointing out the weaknesses in the organizations.
3. Improve the computer ethics rules and regulations by pointing out the weaknesses of current rules and regulations.

3. Research objectives

The major objectives of this research paper are concerned with answering the following questions;

1. What is the effect of *studying computer ethics on computer ethics rules and regulations*?
2. What is the effect of *studying computer ethics on computer ethics at work*?
3. What is the effect of *computer ethics rules and regulations on computer ethics at work*?
4. Is the demographic information (*gender, age, education level, and job position*) having statistically significant differences on *computer ethics at work*?

4. Computer ethics literature review

In mid-1970s, Walter Maner began to use the term "computer ethics" [7]. In 1985, Moor published his known-classic article "What is Computer Ethics?" [8]. In that same year, Deborah Johnson published "Computer Ethics" which was the first textbook in this field [9]. Information ethics is about the critical reflection on the visions and options for better lives in the digital age, not only about norms [10]. The proper control measure should be applied upon identifying the unethical behavior in order to transfer the negative behavior to a more positive behavior. This will be the basement to create a code of computer ethics especially for countries with deficiencies in computer ethics [11]. Security professionals should prevent, detect, and manage malicious insider activity and risk by producing empirically derived results from insider and outsider computer criminal activity [12]. There are two common threats, firstly, the rise of 'hacktivists' or cyber terrorists. The second threat is cybercrime [13, 14].

The dependence on information technology needs a higher standard of cyber security to maintain the availability and integrity of the essential services such as e-banking. This increased the demand skilled for cyber professionals [15].

The Internet and cyberspace are shared between everyone in the world, thus all countries should collaborate, at the international level, to counter the broad range of threats [16]. The lists of definitions of the most popular types of computer crimes are sorted alphabetically in Table 1.

Table 1. Most popular computer crimes

Computer crime type	Source
Carding: is the use of unlawfully obtained credit or debit cards.	[17]
Cloning: is a cellular phone fraud accomplished through computers.	[18]
Data diddling: altering raw data just before it is processed by a computer and then changing it back after the processing is completed.	[19]
Denial of Service (*DoS*): overwhelms the computer and causes it to fail to respond or function for its intended users.	[20]
Dumpster Diving: It does not require any technical expertise, simply has no go through dumpsters (trash) and garbage cans for company documents, credit card receipts, phonebooks, meeting minutes, and other papers containing sensitive information.	[18]
Hype Cycle for Privacy: Security and risk management leaders treating technology, information and resilience risk must place privacy as a top three priority.	[21]
Identity Theft: types of crime in which someone wrongfully obtains and uses another person's personal data.	[22]
Internet Time Theft: an unauthorized person uses Internet hours paid by another person.	[18]
Mail Bombings: the cyber-criminal creates havoc by simply bombarding a person's e-mail address.	[18]
Malware: software that is designed to cause damage to a user's computer, server, or network.	[20]
Phishing: criminals are use spoofed emails and fraudulent websites to trick people into giving up personal information such as usernames, passwords and credit card details.	[23]
Preaching: a crime committed against telephone company, computers with the aim of making free long-distance calls.	[18]
Piggybacking or Shoulder-surfing (*ATM fraud*): the act or prying on others important data to use it later for some benefit is called shoulder surfing.	[18]
Pornography: a crime where material (either pictures or photos or words) appearing on websites.	[18]
Salami Slicing: a form of data diddling, where a small change is made; the alteration is so insignificant that in a single case it can easily go unnoticed.	[18]
Sniffing: a program, which sets the NIC of the targeted computer into such settings that it allows the intruder to capture packets of information.	[18]
Social Engineering: a technique used by hackers or other attackers to gain access to information technology systems by getting the needed information.	[24]
Software Piracy: unauthorized use, duplication, distribution or sale of commercially available software.	[25]
Spoofing: the spoofer uses a program duplicate an organization's login screen.	[18]
Trojan: program that does not self-replicate but takes malicious action on the computer.	[20]
Viruses: programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network.	[19]
Worms: malware that spreads by spontaneously sending copies of itself through email.	[20]

Computer crimes are generally classified into six categories. These categories are military and intelligence attacks, business attacks, financial attacks, terrorist attacks, grudge attacks, and thrill attacks [26].

The number of cybercrime victims is 378 million per year and exceeding a million per day, this indicated for every asecond there are 12 victims. Furthermore, the global cost of cybercrimes was $113 billion; this indicated that half of online adults have been suffered from cybercrimes and/or negative online situations in the past year. Moreover, 41% of them attacked by malware, viruses, hacking, scams, fraud and theft [27]. Best practices on cybercrime prevention need the cooperation across the private sector, communities, government, and internationally. In addition, those good practices must include the promulgation of legislation, effective leadership, the development of criminal justice and law enforcement capacity, education and awareness, the development of a strong knowledge base [28].

To successfully reduce threat, multidisciplinary approach was suggested by involving education of the cyber-citizens and the high-tech CEOs [29, 30]. Dolado [31] found that the computer ethics courses affect the computer ethics of the students, because their feedback on these courses was positive. Ben-Jacob [32] found that the integration of the technology in our lives makes the computer ethics education critical. Many studies recommended computer ethics rules and regulations development to reduce cybercrimes [16, 31, 33, 34], their studies showed the importance of computer ethics rules and regulations to help organizations in reducing cybercrimes.

Information technology (IT) plays a major role in reducing the threats and preventing cybercrimes [35]. All vulnerable businesses using IT such as; banks, insurance, communications/media, defiance contractors, health care, technology, highprofile businesses, financial institutions and governments are at high risk, because of cybercrimes compared to the risks in other sectors [36, 37].

5. Research model and methodology

This paper depends on self-administrated questionnaire. According to Ryu [38] questionnaires are often regarded as an inexpensive and convenient way to collect data from a large number of participants. According to Fanning [39] survey questionnaire is used to collect measurable data from a specific group of people.

The questionnaire was based on the knowledge gained from surveying several literatures (see Table 2). It includes three dimensions, which are studying computer ethics, computer ethics rules and regulations, and computer ethics at work.

Table 2. Literature related computer ethics factors

Computer ethics factors	Supported literature
Studying computer ethics	[15, 31, 32]
Computer ethics rules and regulations	[14, 31, 33]
Computer ethics at work	[31, 36]

The conceptual model of computer ethics factors is shown in Figure 1. The questionnaire consists of two parts, the first part was for demographic information and questions concerning general information; the second part consists of 14 statements divided into three factors measuring the computer ethics. To answer the questions of this paper the following hypotheses were designed.

H_1: *Studying computer ethics* have an effect on *computer ethics rules and regulations*.

H_2: *Studying computer ethics* have an effect on *computer ethics at work*.

H_3: Computer ethics rules and regulations have an effect on computer ethics at work.

H_4: Demographic information (*gender, age, education level, and job position*) have statistically significant differences on *computer ethics at work*.

Questionnaire was validated before using it to test the research hypotheses. The questionnaire statements constructed on a five-point Likert scales with end points of *strongly disagree* and *strongly agree*. To collect data 370 copies of the questionnaires were distributed online and 85 in paper form. The number of online received responses were 321 and 53 were received from the paper version. The total respondents were 374.

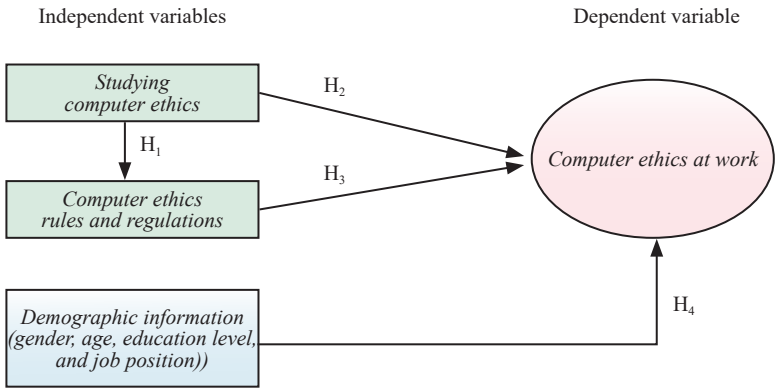

Figure 1. Conceptual research models

The correlation or effect factor between the dimensions calculated to measure the direction and the degree of correlation or effect factor that is rated between –1 and +1. The positive values mean positive correlation or effect factor, while the negative values mean negative correlation or effect factor. Table 3 shows the scale of 5 levels used to measure the strength of the correlation or effect factor as follows [40].

Table 3. Interpreting strengths of correlations

N	Correlation value	Interpretation
1	± 70 or higher	Very strong correlation
2	± < 70 to ± 40	Strong correlation
3	± < 40 to ± 30	Moderate correlation
4	± < 30 to ± 20	Weak correlation
5	± < 20 to ± 01	No or negligible correlation

Source: http://faculty.Quinnipiac.edu/libarts/polsci/Statistics.html

There are many methods for estimating questionnaire reliability, that measures the internal consistency of questionnaire statements. Cronbach's alpha was selected in testing the questionnaire reliability. The test was held to each dimension and for the total statements of the questionnaire. According to Wang [41], the dimension with alpha coefficient value of 0.6 and above will be considered reliable. The results of testing the questionnaire by Chronbach's Alpha showed that all the factors (dimensions) are above 0.6, with overall reliability of 0.822.

6. Data analysis and discussion

6.1 *Descriptive analysis*

The three dimensions of the questionnaire were analyzed by using SPSS. The first dimension is *studying computer ethics*, which consists of 5 statements. The second dimension is *computer ethics rules and regulations* that contain 5 statements. The last dimension is *computer ethics at work*, which consists of 4 statements. Table 4 summarizes averages, standard deviations (SD), and ranking the statements.

The first dimension measured *studying computer ethics*, the highest responses, was for S1: "*Early study of computer ethics will help the new generation to use computer ethically*" with an average value of 4.26 and standard deviation 0.877. The dimension average is 4.038 with standard deviation of 0.956, which is falling in the agree degree of

agreement. From this dimension, it appears that the respondents agreed on the importance of *studying computer ethics*. In addition, this is what Kizza [42] argued, that *studying computer ethics*, including an ethical framework is an argent need. Moreover, the *studying computer ethics* is a long-term investment, especially in the youth to build their character and guide their actions.

The second dimension measured *computer ethics rules and regulations*, the highest responses is for S10 "*Financial department is the most targeted by computer criminals*" with average value of 4.24 and standard deviation of 0.869. The dimension average is 3.848 and standard deviation of 1.013, which is falling in the agree degree of agreement. From the results, it is clear that the respondents agreed on the importance of rules and regulations in financial department and they strongly agreed that the financial department is the most targeted department by computer criminals. They, also, agreed that even if there is availability and awareness of professional codes, norms, laws, etc., many professionals will act unethically, this is clear from S9. And this is what Sembok [34] recommended, establishment of up-to-date, common, and mutually supporting cyber-laws to fight against crimes toward the creation of cybercrime free information society.

The third dimension measured the *computer ethics at work*, the highest responses is on S14 "*It is more secure if the network security is updated frequently*" with an average value of 4.32 and standard deviation of 0.815. The dimension average is 3.818 with standard deviation of 1.031, which is falling in the agree degree of agreement. From the results, it is clear that S13 "*It is easier to find a job if I declare that I act ethically in the professional environment*" got the lowest average. This indicates that the responds have low awareness of computer ethics in the financial department.

Table 4. Averages and standard deviations of the questionnaire statements

Dimension	Statement No.	Statement	Average	SD*	Rank
Studying computer ethics	S1	Early study of computer ethics will help the new generation to use computer ethically.	4.26	0.877	1
	S2	I recommend studying computer ethics course as mandatory course in schools and universities curriculum.	4.04	0.990	2
	S3	Computer ethics study will reduce the computer crimes.	3.95	1.017	5
	S4	It is important to teach computer ethics by lectures or workshops.	3.95	0.922	4
	S5	Learning computer ethics is useful, in my work.	3.99	0.975	3
		1st dimension average	4.038	0.956	-
Computer ethics rules and regulations	S6	The agreement to safely use the computer guarantees the rights and safety of the parties.	3.90	1.002	3
	S7	Commitment to the rules and regulations will reduce the work of computer crime.	4.16	0.883	2
	S8	The only important thing with respect to the professional behavior is the awareness of the law. The ethical aspect is a secondary aspect, unless it has legal consequences.	3.36	1.238	5
	S9	Many professionals will continue to act unethically, even if there is availability and awareness of professional codes, norms, laws, ect.	3.58	1.075	4
	S10	Financial department is the most targeted by computer criminals.	4.24	0.869	1
		2nd dimension average	3.848	1.013	-
Computer ethics at work	S11	I follow computer ethics, when I use computer in my work.	4.25	0.943	2
	S12	A manager trust employee who is under a code of computer ethics than other who is not.	3.78	1.079	3
	S13	It is easier to find a job if I declare that I act ethically in the professional environment.	2.92	1.286	4
	S14	It is more secure if the network security is updated frequently.	4.32	0.815	1
		3rd dimension average	3.818	1.031	-

*SD: Standard deviation

6.2 *Correlation of the dimensions*

The data distribution of the 14 statements of the questionnaire was tested by Kolmogorov-Smirnov, the results of testing shows that the data distribution is not normal. Therefore, Spearman's test for correlation was used to test the correlation between the dimensions of the questionnaire in case of the data distribution is not normal [43]. The results are shown in Table 5. The correlation is strong between "*studying computer ethics*" and "*computer ethics at work*" with value 0.511. Furthermore, it is very clear the correlation between "*studying computer ethics*" and "*computer ethics rules and regulations*" is strong with value 0.447. While the correlation between "computer ethics rules and regulations" and "computer ethics at work" is moderate with a value of 0.324.

From the above it is clear that the weakest correlation was between the dimensions "*computer ethics rules and regulations*" and "*computer ethics at work*" due to the lack of strength rules and regulations and the lack of legal cybercrimes rules in Bahrain.

Table 5. Spearman's correlation matrix questionnaire between dimensions

Dimension	Studying computer ethics	Computer ethics rules and regulations	Computer ethics at work
Studying computer ethics	1		
Computer ethics rules and regulations	0.447**	1	
Computer ethics at work	0.511**	0.324**	1

**. Correlation is significant at the 0.01 level (2-tailed)

6.3 *Hypotheses testing*

The hypotheses (H_1, H_2, H_3) are tested by simple linea r regression as shown in Table 6, the first hypothesis H_1: *Studying computer ethics* have an effect on *computer ethics rules and regulations*. This hypothesis is related to the first dimension that measures *studying computer ethics*. The table shows that the coefficient of determination *r* square equal to 0.20, which indicates that *studying computer ethics* have a weak effect on computer ethics rules and regulations. In addition, the significance level of F (sig) equals to 0.000, which indicates that there is a significant difference between *studying computer ethics* and computer ethics rules and regulations; which affirms that studying computer ethics have an effect on the computer ethics rules and regulations. The regression equation based on the test is given as:

$$\textit{Computer ethics rules and regulations} = 2.34 + 0.374\ (\textit{Studying computer ethics})$$

These results assure that the *studying computer ethics* is important to improve and strengthen the commitment of computer ethics rules and regulations.

The second hypothesis of the study H_2: *Studying computer ethics* have an effect on *computer ethics at work*. From the table, it is clear that *studying computer ethics* have a weak effect on computer ethics at work because the coefficient of determination *r* square value was 0.261. Moreover, the significance level of F (sig) value is 0.000, which indicates that there is a significant difference between *studying computer ethics* and the *computer ethics at work*; which affirms that *studying computer ethics* have an effect on computer ethics at work. The regression equation based on the test is given as:

$$\textit{Computer ethics at work} = 1.76 + 0.509\ (\textit{Studying computer ethics})$$

These results assure that improving *studying computer ethics* is very important to improve and strengthen *computer ethics at work*. For example, most of the information technology users assure that the computer ethics study will reduce the computer crimes. In addition, most of them agreed that learning computer ethics is useful in their work. Furthermore,

they agreed on the need of studying computer ethics either in universities or by workshops.

The third hypothesis of the study H_3: *Computer ethics rules and regulations* have an effect on *computer ethics at work*. The table shows that the coefficient of determination *r* square value is 0.105, which indicates that there is a weak effect of *computer rules and regulations on computer ethics at work*. On the other hand, the significance level of F (sig) value is 0.000, which indicates that there is a significance differences between computer ethics rules and regulations and computer ethics at work; which affirms that *computer ethics rules and regulations* have an effect on *computer ethics at work*. The regression equation based on the test is given as:

Computer ethics at work = 2.33 + 0.385 (*Computer ethics rules and regulations*)

These results assure *computer ethics rules and regulations* are very important to improve and strengthen *computer ethics at work*. For example, commitment to the rules and regulations will reduce computer crimes. Moreover, most of the responds agreed that the only important thing to the professional behavior is the awareness of the law and the ethical aspect is a secondary unless it has legal consequences. Thus, if there are strong rules and regulations toward computer ethics it will have an effect on the computer ethics and will reduce the computer crimes.

Table 6. Regression test for the hypotheses H_1, H_2, H_3

Hypothesis	Source of variance	Sum of squares	df*	Mean square	*r*	*r* square	F	Sig.
H_1	Regression	28.899	1	28.899	0.447	0.199	92.631	0.000
	Residual	116.056	372	0.312				
	Total	144.955	373					
H_2	Regression	53.543	1	53.543	0.511	0.261	131.657	0.000
	Residual	151.286	372	0.407				
	Total	204.829	373					
H_3	Regression	21.524	1	21.524	0.324	0.105	43.680	0.000
	Residual	183.305	372	0.493				
	Total	204.829	373					

df*: Degree of freedom

The hypothesis H_4 used to test the effect of demographic information on *computer ethics at work*. H_4: Demographic information (*gender, age, education level, and job position*) have statistically significant differences on *computer ethics at work*. Table 7 shows there is statistically significant difference on *computer ethics at work* according to gender because the sig value is less than (α = 0.05). The result indicates that the average of female in the study were greater than males. This is similar to what Dalton and Ortegren (2011) argued, that a large number of studies find that females report more ethical responses than males and this is corresponding with the result of the this paper.

Table 7. T-test for gender

Dimension	Gender	N	Mean	SD	Std. error mean	t	Sig.
Computer ethics at work	Male	260	3.788	0.793	0.049	-1.157	0.009
	Female	114	3.884	0.603	0.057	-1.285	

Table 8 shows the results of variance analysis by one way Analysis of Variance (ANOVA) according to *age, education level*, and job postion. The table shows that the age has statistically significant difference on *computer ethics at work*, because the sig value is less than ($\alpha = 0.05$). Therefore, Scheffe test was used to find the sources of differences between the groups of *age*. The results of Scheffe test showed that there is no statistically significant differences between *age* groups and *computer ethics at work*, the differences between their averages are likely due to chance and not likely due to the independent variable manipulation. The table shows that the *education level* and *job position* has no statistically significant differences on the *computer ethics at work* since the sig values of these dimensions are greater ($\alpha = 0.05$). On the other hand, position has statistically significant influence on computer ethics rules and regulations since the sig value is less than ($\alpha = 0.05$). Therefore, Scheffe test was used to find the sources of differences between the groups of position and computer ethics rules and regulations.

Table 8. Variance analysis for age, education level, and job position

	Age		Education level		Job position	
Dimension	F	Sig.	F	Sig.	F	Sig.
Computer ethics at work	5.889	0.000	1.871	0.134	1.600	0.174

7. Conclusions

Most of the public and private organization are providing online services to its users to facilitate the use of online services easily and rapidly. This paper evaluated the effect of studying computer ethics and computer ethics rules and regulations on computer ethics at work. A self-administrated questionnaire was designed to employees working in different organizations in Bahrain. According to the opinions of the questionnaire respondents, studying computer ethics early is a must to help the new generation to use computer and internet ethically, as well as the rules and regulations played very important role on computer ethics at work.

Almost all the respondents gave positive responses towards the importance of rules and regulations to reduce computer crimes. The gender and age played an important role on *computer ethics at work* because, the new generation of employees maybe learned computer ethics either at schools or at colleges. While the level of education level and the job position have no statistically effect, because the employees following regulation of computer ethics at work are very important to employees regardless to their level of education level or job position, therefore they need continuous learning through workshops, to update their information regarding information technology crimes.

According to the results of this study, the study recommended; giving intensively interest in educating employees and increasing their awareness to computer ethics and computer crimes by holding courses and workshops periodically.

Conflict of interest

The author declares no competing financial interest.

References

[1] Bynum T. *Computer and information ethics*. Available from: https://plato.stanford.edu/archives/win2014/entries/ethics-computer/ [Accessed 1st July 2020].
[2] Kuzu A. Problems related to computer ethics: origins of the problems and suggested solutions. *Turkish Online Journal of Educational Technology*. 2009; 8(2): 91-110.
[3] Kroger DJ, Sena MP. An MBA course in ethics, security, and privacy. In: *The Proceedings of ISECON*. 2002.
[4] Lim J, Hwa NK. Computer fraud and ethics: the societe generale's trading fraud. In: *2011 International Conference*

on Computer and Management (CAMAN). IEEE; 2011. p.1-3.
[5] Akbulut Y, Odabasi HF, Kuzu A. Computer ethics: scenes from a computer education department in turkey. In: *Ethical Practices and Implications in Distance Learning*. IGI Global; 2009. p.295-304.
[6] Central Bank of Bahrain. *Announcement*. 2019. Available from: https://www.cbb.gov.bh/ar/page_1.php?p=%D8%A8%D9%8A%D8%A7%D9%86_%D8%B5%D8%AD%D9%81%D9%8A [Accessed 1st July 2020].
[7] Bynum TW, Rogerson S. *Computer Ethics and Professional Responsibility*. Oxford UK: Blackwell Publishing; 2004.
[8] James HM. What is computer ethics? *Metaphilosophy*. 1985; 16(4): 266-275.
[9] Johnson DG. *Computer Ethics*. Englewood: Prentice-Hall; 1985.
[10] Capurro R, Britz JB. In search of a code of global information ethics: the road travelled and new horizons. *Ethical Space: The International Journal of Communication Ethics*. 2010; 7(2): 28-36.
[11] Aziz AA, Lokman AM, Yusof ZM. Information technology ethics: the conceptual model of constructs, actions and control measure. *International Journal on Computer Science and Engineering*. 2011; 3(6): 2580-2588.
[12] Cummings A, Lewellen T, McIntire D, Moore AP, Trzeciak RF. *Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector*. Software Engineering Institute; 2012.
[13] Davis S. Is your company managing data effectively? *Premium Magazine*. 2013. Available from: https://premium-me.com/lander [Accessed 1st July 2020].
[14] Christoph S, Pavan D. *Cyber Ethics 4.0: Serving Humanity with Values*. 2018.
[15] Australian Government. *Australia's 2020 cyber security strategy, commonwealth of Australia*. 2019. Available from: https://www.enisa.europa.eu/topics/nis-directive [Accessed 1st July 2020].
[16] Singh S, Gupta P. Cyber crime and legal issues. In: Jaishankar K, Ronel N. (eds.) *Proceedings of the Second International Conference of the South Asian Society of Criminology and Victimology*. India; 2013. p.437-439.
[17] Seger A. Cyber crime and economic crime. In: Edelbacher M, Kratcoski P, Theil M. (eds.) *Financial Crimes: A Tthreat to Global Security*. New York: CRC Publishing; 2012.
[18] Pardesi JD. *Emerging Trends in Information Technology*. Nirali Prakashan; 2007.
[19] Rathinasabapathy G, Rajendran L. Cyber crimes and information frauds: emerging challenges for LIS professionals. In: *Information to Knowledge: Technology and Professionals. Proceedings of the Conference on Recent Advances in Information Science and Technology.* Kalpakkam: MALA and IGCAR. 2007. p.131-142.
[20] Microsoft. *Microsoft Security Intelligence Report*. 2014. Available from: http://www.microsoft.com/security/sir/default.aspx [Accessed 1st July 2020].
[21] Gartner. *Hyper cycle privacy, 2019*. Available from: https://www.gartner.com/en/documents/3947373 [Accessed 1st July 2020].
[22] Knox J. *Identity theft and identity fraud*. 2014. Available from: https://www.justice.gov/criminal/fraud/websites/idtheft.html [Accessed 1st July 2020].
[23] Chaudhary G. Development review on phishing: a computer security threat. *International Journal of Advance Research in Computer Science and Management Studies*. 2014; 2(8): 55-64.
[24] Orgill GL, Romney GW, Bailey MG, Orgill PM. *The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems*. Salt Lake City: ACM; 2004.
[25] Moores T, Dhillon G. Software piracy: a view from Hong Kong. *Communications of the ACM*. 2000; 43(12): 88-93.
[26] Stewart JM, Chapple M, Gibson D. *CISSP: Certified Information Systems Security Professional Study Guide*. John Wiley & Sons; 2012.
[27] Norton. *Norton Report*. Norton by Symantec. 2013. Available from: https://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013/ [Accessed 1st July 2020].
[28] United Nations Office on Drugs and Crime. *Comprehensive study on cybercrime*. Available from: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf [Accessed 1st July 2020].
[29] Magnin CJ. *The 2001 council of europe convention on cyber-crime: an efficient tool to fight crime in cyber-space*. Santa Carla University, USA; 2001.
[30] Tzafestas SG. Ethics and law in the internet of things world. *Smart Cities*. 2018; 1(1): 98-120.
[31] Dolado J. Is it worthwhile to teach computer ethics. In: Georgiadou E, King G, Pouyioutas P, Ross M, Staples G, Inspire V. (eds.) *Quality and Software Development: Teaching and Training Issues*. UK: The British Computer Society; 2000.
[32] Ben-Jacob M. Integrating computer ethics across the curriculum: a case study. *Educational Technology & Society*.

2005; 8(4): 198-204.
[33] Arenas MT. *Social Engineering and Internal Threats in Organizations*. 2008.
[34] Sembok T. *Ethics of Information Communication Technology*. Regional unit for social and human sciences in asia and the pacific, unesco; 2004. p.239-325.
[35] Fatima A. E-banking security issues-is there a solution in biometrics? *Journal of Internet Banking and Commerce*. 2011; 16(2): 1-9.
[36] Franzke A, Bechmann A, Zimmer M, Ess CM. *Internet research: ethical guidelines 3.0*. Available from: https://aoir.org/reports/ethics3.pdf [Accessed 1st July 2020].
[37] Suja P, Raghavan N. Cybercrime in banking sector. *International Journal of Research in Social Sciences*. 2014; 4(1): 189-194.
[38] Ryu YS. *Development of usability questionnaires for electronic mobile products and decision making methods.* Virginia, USA; 2005.
[39] Fanning E. Formatting a paper-based survey questionnaire: best practices. *Practical Assessment Research & Evaluation*. 2005; 10(12): 1-14.
[40] Pearson's r Correlation. 2015. Available from: https://faculty.Quinnipiac.edu/libarts/polsci/Statistics.html [Accessed 1st July 2020].
[41] Wang R. *Relationship, Loyalty, and Marketing-A Correlation Study of Taiwan Hotel Customers' Perspectives*. Oklahoma State University; 2007.
[42] Kizza JM. *Ethical and Social Issues in the Information Age*. London: Springer; 2013.
[43] Devore J, Farnum N, Doi J. *Applied Statistics for Engineers and Scientists*. 3rd ed. Cengage Learning; 2013.