A Survey on the Ethical Use of Information System in IT Company and Business Organization in the context of Bangladesh

Rezvi Shahariar
Institute of Information Technology
University of Dhaka
rezvi@du.ac.bd

Shuvradeb Saha
IIT, University of Dhaka
bsse0815@iit.du.ac.bd

Aba Kawser Tusher
IIT,University of Dhaka
bsse0825@iit.du.ac.bd

Suravi Akhter
IIT, University of Dhaka
bsse0827@iit.du.ac.bd

Abstract- This paper report is about the ethical issues while using information system in IT company and business organization in Bangladesh. The discussion topics are covered by purpose of using information system, issues of privacy, use of company software for personal gain and integrity of intellectual property and confidentiality agreements. Data were collected via questionnaire.

The results show that how much organization is aware and promised in using information system ethically and ensure privacy and confidentiality of customer data.

Keywords- information system; data privacy; confidential data; information system security

1. Introduction

Use of information system is growing rapidly in office automation, e-business and banking etc. Although the information system increases performance in the workplace, we must be aware of the factors that will be a direct impact on information system security. Mazon identified four issues of particular concern while using information system. At first, Information systems should not unduly invade a person's privacy. Second one is the information system must be accurate. Third one is information system should protect the intellectual property of individuals as well as the infrastructure through which the information flows. And the last one is the information systems must be accessible by all to ensure ability to participate in society. [1] There is a long history of research on ethics and computing going back to the very development of digital computers (Wiener, 1954). [2] The scope of ethics in Information System is wide and can include topics such as privacy, intellectual property, employment relationships, design decisions, or the changing role of humans in society. Many or most aspects of IS are either influenced by ethical views or they can have an influence on rights, obligations, or utilities. The current paper aims to improve the quality of ethics-related IS research by discussing some of the main and recurring issues. Such guidance is much-needed; in particular because many Information System scholars who have an interest in ethics have only limited knowledge of the extensive literature on ethics as moral philosophy. At the same time such work can raise considerable problems in its own right. Among them there are ethical issues arising from potential regulations on research on ethics. The current paper is constructed as a set of questions, rather than an algorithmic piece of advice. Each of these questions requires careful deliberation and explicit reasoning. Most of them are of relevance for research not concerned with ethics but the concept of ethics raises particular angles. Not all of the questions will have to be answered expressly in each piece of research as the answer will in many cases be implicit. This

implicit nature on the view of some of these questions can be problematic.

This paper is about the ethical issues is raised by information systems and explore and study those factors.

2. Background Study

Conducting this research we need to study details about the information system, the ethical issues while using information system and the professional code of ethics.

- **Information System:** Many organization works with large amounts of data. Data are basic values or facts and are organized in a database. Many people think of data as synonymous with information; however, information actually consists of data that has been organized to help answers questions and to solve problems. An information system is defined as the software that helps organize and analyze data. So, the purpose of an information system is to turn raw data into useful information that can be used for decision making in an organization
- **Data Privacy:** Data privacy, also called information privacy, is the aspect of information technology (IT) that deals with the ability an organization or individual has to determine what data in a computer system can be shared with third parties. [3] Data privacy and data protection are very closely interconnected, so much so that users often think of them as synonymous. But the distinctions between data privacy vs. data protection are fundamental to understanding how one complements the other. Privacy concerns arise wherever personally identifiable information is collected, stored, or used.
- **Data integrity:** Data integrity refers to the accuracy and consistency of data stored in a database, data warehouse, data mart.
- **Confidentiality:** Confidentiality is the protection of personal information. Confidentiality means keeping a client's information between you and the client, and not telling others including co-workers, friends, family, etc.

  Examples of maintaining confidentiality include:

  - Individual files are locked and secured
  - Support workers do not tell other people what is in a client's file unless they have permission from the client
  - Information about clients is not told to people who do not need to know
  - Clients' medical details are not discussed without their consent
  - Adult clients have the right to keep any information about them confidential, which includes that information being kept from family and friends. [4]

3. The ethical issues within the context of information system

Individual background, knowledge, belief and thoughts vary person to person. As the same way the industry standards vary organization to organization though many laws, regulations and industry standards is similar within the business and IT Company. For this reason ethics will not get an accurate conclusion of right and wrong. [5] It depends on the authority, organization, laws, rules, regulation and environment of the company. The main issues is the organization and customer data privacy, unauthorized access, using information system for personal benefits, integrity of customer organization agreement.

3.1 Several aspects of ethical issues in information System

By viewing technically, the ethical issues include privacy, accuracy, accessibility, property and occupational health as well. [6]

Privacy is the main issue in using information system. Privacy means the ability to of an organization or individual to determine the limited access from third party and hiding internal information from competitors and unauthorized person. Data privacy policies are strictly maintained while using information system though sometimes data leakage is occurred. The second ethical issue is the accuracy of the information. Accuracy is the correctness of the information/data is provided by the organization/customer. Information system may provide error data if the user is not aware. For example user may provide incorrect data. Each information system must ensure the access limitation by user level and unauthorized access. Currently, some systems monitor the employee during their work time. They also monitor the employee email, phone calls and internet records. The employee privacy is disclosed due to company rules.

Though information system increase the workplace performance in the organization sometimes improper use of the system can cause harm or damage to the society, human life and even the country. Organization must give serious attention in the information system ethics.

3.2 Professional code of conduct

IT company and business organization follows professionals and moral norms and ethical standards. Institute of electrical and electronics engineer (IEEE) recommended some code professional code of ethics. These code of ethics describe precisely below-

As an IT professional, he should follow the following ethical behaviors

1. **Contribute to society and human well being.**

The basic instinct of all life is self preservation. This results in self-oriented thinking and actions. By socialization we inculcate of ethical values and the person learns the merits of cooperative behavior and widens his perception. If there was a decline of ethical behavior in the society, it would lead to trouble. People might indulge in self aggrandizement, corruption, disregard environment damage etc. Though this might in the short run seem beneficial and profitable, in the long run it would be detrimental to the individual as well as community.

2. **Avoid harm to others.**

"Harm" means negative consequences such as undesirable loss of information, loss of property, damage or unwanted environmental impacts. Example of harms includes unjustified physical or mental injury, unjustified destruction or disclosure of information, unjustified damage to property, reputation and the environment. For minimizing the possibility of indirectly harming others, computing professionals must minimize malfunctions by using information system. If the system features are misrepresented to users, coworkers or supervisors, the individual computing professional is responsible for any resulting injury.

3. **Be honest and trustworthy**

Being trustworthy is admirable and desirable. It's a trait other people look for in a person and its confirmation that you're reliable, supportive and honest. A computing professional should be transparent and provide full disclosure of all potential problems to the appropriate parties.

4. **Be fair and take action not to discriminate.**

Inequities between different groups of people may result from the use or misuse of information and technology. In a fair society, all individuals would have equal opportunity to participate in, or benefit from, the use of computer resources regardless of

race, sex, religion, age, disability, national origin or other such similar factors.

5. **Respect the work required to produce new ideas, inventions, creative works, and computing artifacts.**

Developing new ideas, inventions, creative works, and computing artifacts creates value for society, and those who expend this effort should expect to gain value from their work. Computing professionals should therefore credit the creators of ideas, inventions, work, and artifacts, and respect copyrights, patents, trade secrets, license agreements, and other methods of protecting authors' works.

6. **Respect privacy.**

Computing professionals should only use personal information for legitimate ends and without violating the rights of individuals and groups. This requires taking precautions to prevent re-identification of anonymous data or unauthorized data collection, ensuring the accuracy of data, understanding the provenance of the data, and protecting it from unauthorized access and accidental disclosure.

7. **Honor confidentiality.**

Computing professionals are often entrusted with confidential information such as trade secrets, client data, nonpublic business strategies, financial information, research data, pre-publication scholarly articles, and patent applications. Computing professionals should protect confidentiality except in cases where it is evidence of the violation of law, of organizational regulations, or of the Code. [7]

4. Methodology

Methodology is the process in which approach the project is done.

4.1 Research Design

A research design is the set of methods and procedures used in collecting and analyzing measures of the variables specified in the research problem research.

First step, determine the project topic and make a proposal based on this topic. **Second step,** make the questionnaire which is required for project requirement. **Third step**, collecting the data from the organization. **Fourth step** analyze the data and conclude a decision. And the last is the **Fifth step**, survey report is prepared.

4.2 Data collection Resources

In a survey, data can be collected in two ways. First one is primary data resources and the second one is the secondary data resources. [9] Data is collected by using primary data resources and via the questionnaire. Primary data is data that is collected by a researcher from first-hand sources, using methods like surveys, interviews, or experiments. Secondary data refers to data which is collected by someone who is someone other than the user. Common sources of secondary data for social science include censuses, information collected by government departments, organizational records and data that was originally collected for other research purposes. Data is collected from IT company and the business organization which include Cefalo Bangladesh Limited, MJL Bangladesh Limited, Active IT Zone, Orion Informatics Ltd., WhiteSpot Digital Ltd., Islami Bank Bangladesh Limited (IBBL), Sonali bank Limited, Janata bank limited, Agroni bank limited etc.

4.3 Survey Method

The essence of survey method can be explained as "questioning individuals on a topic or topics and then describing their responses" [10]. Survey method can be broadly classified into three categories: interviews, questionnaire and documentation reviews. Using questionnaire and interview technique data is collected.

4.4 Survey Findings

From our survey we have gathered some information about the information systems in various organizations.

- What are the types of Information Systems used in your organization?

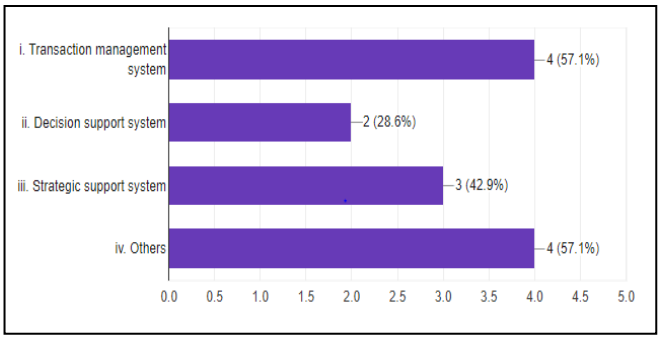

Figure 1: Usage scenario of information system

them use Transaction management systems. Some organizations are using each of the information systems. Here the others information system are expert systems and neutral networks.

- Are there any training courses for employees for using information systems?

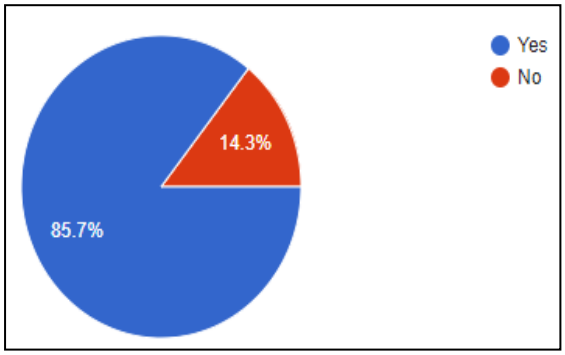

Figure 2: Employee training courses

This figure indicates that most of the organizations arrange training courses for the employees for using the information systems. About 85.7% of the organization arrange training program on information system

- Is there any possibility of confidential data leakage from the information system?

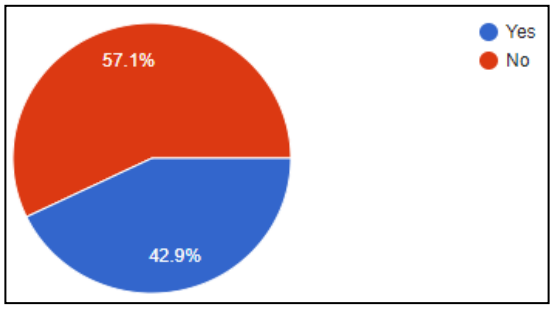

Figure 3: Confidential data leakage from information system

According to our survey most of the organizations have the possibility of confidential data leakage from the information system. About 57.1% of the organizations have faced the problem of confidential data leakage.

- Have any obligation to respect and protect the integrity of intellectual property and confidentiality agreements?

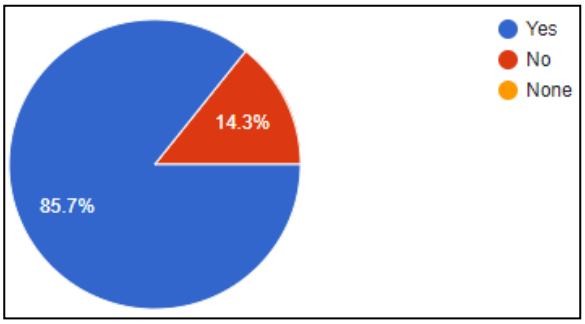

Figure 4: Integrity of intellectual property and confidentiality agreements

From the above figure we see that 85.7% of the organization have obligation to respect and protect the integrity of intellectual property and confidentiality agreements.

- Should employees not disclose confidential organizational information to co-workers without authorization?

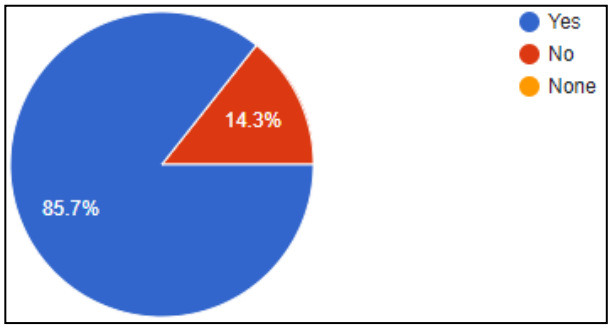

Figure 5: Disclosure of confidential organizational information

Almost all the organizations are agreed with not disclosing confidential organizational information to co-workers without authorization.

- Should not violate the privacy and confidentiality of information entrusted to me to further personal interest?

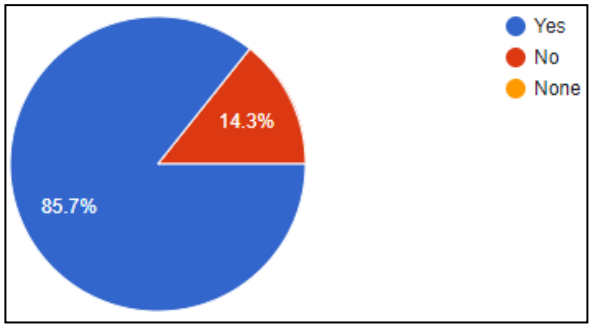

Figure 6: Privacy and confidentiality of information

Most of the organizations agreed with not violating the privacy and confidentiality of information entrusted to them to further personal interest.

- Which ethical issues are maintained while using information system? What are the rules while using information system?

Ethical issues are maintained while using information system is:

1. Prevent hacking
2. Information privacy, Customer data security, Non Disclosure Agreement
3. Security & Integrity
4. Confidentiality & Security
5. Transparency & Security
6. Data encryption

Role of using information system are:

1. Minimizing cost & time
2. Confidentiality should be maintained
3. None is allowed to share any official information with others. To access official documents or templates each employee must ask for permission to the admin through the system for a certain period of time.
4. Don't store "Non public personal information" if it isn't a must. If you store that kind of information, if you can, store value if possible. No developer can have access to production database.

- How do you prevent unauthorized access? If any unauthorized access occurs what step you take?

The methods of preventing unauthorized accesses are:

1. Using IP filtering and authorization key
2. By maintaining desktop policy
3. Implementing secured network and information system
4. Authentication and authorization
5. Using antivirus and anti phishing software

The steps taken if unauthorized access occurs are:

1. Shutting down the affected server and providing service via backup server.
2. Block particular user from system
3. Taking legal action

5. Recommendation

Nowadays information system has become a buzzword in IT industry, bank or any other corporate or social organization. Although with the help of information system the organization

can perform many complicated decisions about that organization. But there are some security threats of using information system. There are some issues that are related with that. The technical information and rationality, the habits of using information system, the employee's level of education are affecting the security of information system. Apart from these the employee's cultural, ideological and ethical standards are also responsible for security threat of information systems.

A. Improving training program

Now most of the information system has become computer based. And in the context of our country it's highly necessary to arrange advanced training program for the employee's as most of our people are not technically sound. The ethical code of conducts that should be maintained using information system must be added in the training program. Enhance the education for the information system engineers and end users.

B. Rationality in Information system

- Advanced technology should be used to keep the information system secured. The information system security which is more commonly referred to as INFOSEC, refers to the processes and methodologies involved with keeping information confidential, available and assuring its integrity [11]. For example: using the encryption and decryption technology to protect the information and communication details from unauthorized user; using user classification technique to set users authority and restrict users to freely modify the system and access to confidential data; setting a period based access system so that user can access to the system till a valid period.
- The data of information system should be collected and preserved in the legal way. Fair information practices are very important today. The Fair Information Practice Principle (FIPPs) was first published in Records, Computers and the Rights of Citizens: A Report of the Secretary's Advisory Committee on Automated Personal Data Systems. The fundamental principles are:

1. There must be no personal-data record-keeping systems whose very existence is secret.
2. There must be a way for individuals to find out what information about them is in a record and how it is used.
3. There must be a way for individuals to prevent information about them that was obtained for one purpose from being used or made available for other purposes without their consent.
4. There must be a way for individuals to correct or amend a record of identifiable information about them.
5. Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data [12].

C. Industry Standards and Self-Discipline of Employees

Each organization should create its own ethical code of conducts and the employees should maintain the code of conducts. As information system carries much confidential information about the organization, its security should be one of the most important tasks for the manager. Managers can not focus only on technology and tasks, while ignoring people and human rights.

D. Recovering Lost Information

Sometimes important information can be removed accidently so organization must have the way to recover that data. For this they may maintain remote database server where they keep all the data. If the local data somehow deleted accidently they can recover that from the remote database server. Every organization should have any of the following method to recover data after lost-

1. Data Backups
2. Data redundancy
3. Memory restores
4. Block chain

E. Preventing Unauthorized access

Information system contains confidential data leakage of which can be harmful for the organization. So preventing unauthorized access is mandatory. IP filtering can be a great way to control unauthorized access. The information system engineers should implement secured authentication system. They may use popular authentication methodologies that are already in the market.

6. Conclusions

Although the information systems are helping a lot in the organization, it has a lot of drawbacks in the case of information security. But the awareness of the users can make it possible to remove those drawbacks. From the arguments laid out above, it follows that there is a need to increase awareness, interest and action concerning the ethical dimension of Information Systems both as a discipline and as a practice. There is opportunity for multidisciplinary dialogue which will promote greater attention to these issues.

7. References

[1] Adman, P. and L. Warren (2000). "Participatory sociotechnical design of organizations and information systems–an adaptation of ETHICS methodology". Journal of Information Technology. 15(1): 39–51.

[2] Adam, A. Gender, Ethics and Information Technology. Basingstoke: Palgrave McMillan, 2005.

[3] Techterget network, https://searchcio.techtarget.com/definition/data-privacy-information-privacy (Last access 07/10/2018)

[4] sielearning education , https://sielearning.tafensw.edu.au/MCS/CHCAOD402A/chcaod402a_csw/knowledge/confidentiality/confidentiality.htm (Last access 07/10/2018)

[5] J. Jiang, Computer systems, database systems and communications network security and confidentiality, University of Electronic Science and Technology Publishing House: Chengdu, China, 1995, pp.375.

[6] Ethics in information technology, Third edition, George W. Reynolds.

[7] Techopedia , https://www.techopedia.com/definition/24840/information-systems-security-infosec (Last access 07/10/2018)

[9] Cyfer data colletion, https://cyfar.org/data-sources (Last access 07/10/2018)

[10] Worldprivacy, https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/ (Last access 07/10/2018)

[11] Techopedia definition, https://www.techopedia.com/definition/24840/information-systems-security-infosec (Last access 07/10/2018)

[12] Endingthedocumentgame, https://endingthedocumentgame.gov/PDFs/Privacy.pdf (Last access 07/10/2018)