A Review on Security versus Ethics

Bisma Bashir
Department of Computer Science & Engineering,
Jamia Hamdard,
New Delhi, India

Aqeel Khalique
Department of Computer Science & Engineering,
Jamia Hamdard,
New Delhi, India

ABSTRACT
Security is of major concern in Information & Communication Technologies (ICT). Valuable data and information must be protected from attackers. In ICT, information is easily accessible and thus efficient security mechanisms are employed to prevent any attack. This paper presents a review about the security and ethics, their relationship with each other. This paper focuses on implementing security mechanism complying ethical best practices. Existing security mechanism and ethical practices in an ICT organization are also discussed in this paper. The paper also covers impact of technologies on the privacy of people due to unawareness of security policies or false ethical practices.

General Terms
Security, Ethics, Ethical Computing, Information & Communication Technologies.

Keywords
Security, Computer Ethics, Ethical Computing, Privacy, Ethical Hacking, Hacking.

1. INTRODUCTION
In today's world, security is much needed because of incremental growth in technology and ease of access to that technology. Security is the protection from any danger, threat, harm etc. Every valuable asset needs to be secure. Confidential data must be secure from unauthorized users. Data must be made available to right person at the right time and in right format without any ambiguity. Security protects information system from data loss, misuse or damage to the hardware and software such as credit card users need to secure their online transaction, etc. Security gives protection against network attacks, code injection, intentional or accidental attacks etc. Security services such as confidentiality, integrity and availability, provides us adequate security. There are many people who try to break into network and computer and steal valuable data and information or damage the system, this act is known as computer crime or cybercrime. Several categories of people who conduct cybercrime are generally known as hackers, cracker, cyber terrorist, cyber extortionist, unethical employee, script kiddies, corporate spy etc.

Valuable data and information become more secure from any attack and threat to that valuable data and information may be reduced if there is proper compliance to ethical practices while implementing security mechanisms. Therefore, security and ethics can be related as shown in Figure 1.

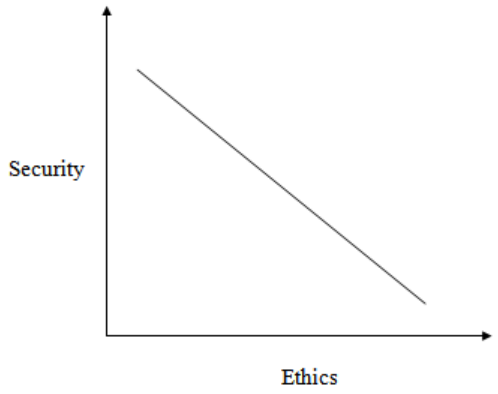

Fig 1: Relationship Between Security And Ethics

Ethics is basically a branch of philosophy which defines moral behavior, moral concepts and moral language. Ethics marks a line between good and bad. Various philosophers such as Socrates, Plato pose various theories which elaborate the guidelines of ethical behavior. When we talk about ethics, we can say that ethics is everywhere. People try to follow these ethics in order to avoid any dilemmas. Ethics helps us to make a decision we can be proud of [1].

This paper presents a relationship between security and ethics applied in technological domain. In this paper, discussion about the security and security services is done in Section 2. Ethics, rules of ethics, and computer ethics are discussed in Section 3. Computer security ethics and ethical hacking is discussed in Section 4. Section 5 discusses about security based ethical issues of an organization, impact of technology on the privacy of people. In Section 6, we do analysis based on the review study of the topic and conclusion in Section 7.

2. SECURITY
Security can be defined as the protection offered to an automated information system in order to attain the applicable objectives of preserving the confidentiality, integrity and availability of information system resources (includes hardware, software, firmware, information/data and telecommunication) [2]. Security mainly consists of confidentiality, integrity and availability and they are referred as security attributes, properties, goals, basic building blocks etc., these security attributes are shown in Figure 2.

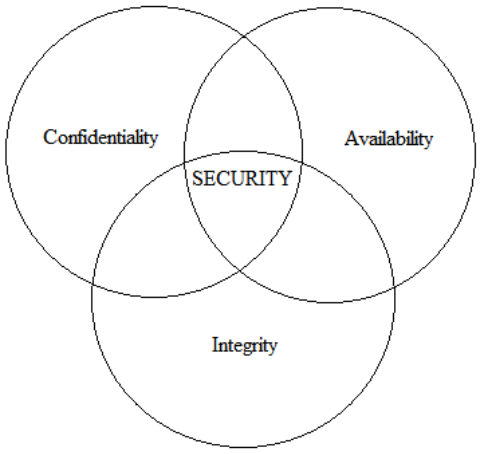

Fig 2: Security Attributes

3. ETHICS

Ethics can be defined as rules and regulations that have been formed to allow an individual to work in accordance to moral principles. Activities done by individuals are governed by ethics. In every organization there are some ethics which must be followed by every user. By acting in accordance to the ethical code, there will be less disruption in an organization. If the employees of an organization do not follow the ethics, then there will be adverse effect on both organization and on employees. The behavior of individual depends on the moral values and ethical practices followed by them. It also enables them to distinguish between right and wrong [3].

The English word ethics is derived from an ancient Greek word ethikos, which means "relating to one's character". This adjective is derived from another Greek word, ethos meaning "character, disposition" [4].

Doing whatever society accepts does not mean we are ethical. Sometimes the whole society can become unethical and corrupted. However, if being ethical were doing "whatever society accepts," then one would find out what society accepts, instead of what is ethical.

3.1 Rules of Ethics

In ethics, the philosophical principle lay down the foundations of morality. These principles are considered as rules of ethics. These rules or philosophical concepts are words of wisdom of great philosophers of ancient world. These rules are stated as follows:

- *"Do unto others as you would have them do unto you"* (the Golden rule) [5]. Putting yourself into the place of others, and thinking of yourself as the object of the decision, can help you think about fairness in decision making.
- *"If an action is not right for everyone to take, it is not right for anyone*" (Immanuel Kant's Categorical Imperative) [6]. Ask yourself, "if everyone did this, could the organization, or society, survive?"
- *"If an action cannot be taken repeatedly, it is not right to take at all"* (Descartes rule of change) [7]. This is the slippery-slope rule: An action may bring about a small change now that is acceptable, but if it is repeated, it would bring unacceptable changes in the long run. In the vernacular, it might be stated as *"once started down a slippery path, you may not be able to stop"*
- *"Take the action that achieves the higher or greater value"* (the Utilitarian Principle) [8]. This rule assumes you can prioritize values in a rank order and understand the consequences of various courses of action.
- *"Take the action that produces the least harm or the least potential cost"* (Risk Aversion Principle) [9]. Some actions have extremely high failure costs of very low probability (e.g., building a nuclear generating facility in an urban area) or extremely high failure costs of moderate probability (speeding and automobile accidents). Avoid these high-failure-cost actions, paying greater attention obviously to high-failure-cost potential of moderate to high probability.
- Assume that virtually all tangible and intangible objects are owned by someone else unless there is a specific declaration otherwise. *"If something someone else has created is useful to you, it has value, and you should assume the creator wants compensation for this work"* [10]. This is the ethical "no free lunch" rule.

3.2 Computer Ethics

As discussed above, those 6 rules are generic rules of ethics. Based on these 6 rules Ten Commandments of computer ethics were created in 1992 by the computer ethics institute. The basic rules of ethics are as under [11]:

- Computer should not be used to harm anyone.
- Computer should not be used to interfere in others work.
- Computer should not be used in stealing data.
- Computer should not be used to bear false witness.
- Pirated software should not be used.
- Without proper authorization one should not use others computer resources.
- Social consequences of the program being developed by you must be taken into consideration.
- One should not appropriate other people's intellectual output.
- Computer should be used in a way that ensures consideration and respect for your colleagues.
- One should not use computer to snoop into others computers.

4. COMPUTER SECURITY ETHICS

As technology progressed, data breach also increased. Network and computers became more prone to attacks. Network and computers must be protected from attack, data loss, misuse theft etc. For example, customers must secure their online transaction and must keep their credit card numbers safe. Computer security risk is any action that could cause loss of information to software, data, processing incompatibilities or damage to computer hardware. A branch of computer security is known as computer crime. Computer crime is slightly different from cybercrime. An illegal act based on internet is known as cybercrime. Several categories of people that carry on cybercrimes are hackers, crackers, cyber terrorist, cyber extortionist, unethical employee, script kiddies, corporate spy etc. These categories are described below [12]:

- A **hacker** is defined as a person who unlawfully uses computer to gain unauthorized access to computer or computer network. Hackers often claim that they do hacking in order to find out loopholes in a network.
- **Cracker** is a person, who intentionally access computer or computer network. Their intentions are not good. They try to steal or destroy the information. Crackers and hackers have advanced network skills.
- **Cyber terrorist** is a person who uses the computer network or internet for political reasons to destroy the computer system. It requires highly skilled persons, lot of money to implement and years of planning.
- **Cyber extortionist** is a person who uses email as an offensive force. They threaten a company by sending a threatening email stating that they will attack company's security or release confidential information of company. They demand a certain amount of money in exchange for not launching an attack.
- An **unethical employee** is a person who unlawfully accesses the company's network, so that he could steal top secret information of the company or want to take revenge.
- **Script kiddies** are similar to crackers because they might want to do harm, but they lack the technical skills. They use prewritten cracking programs.
- A **corporate spy** is a person who has great computer and network skills and they are hired so that they can break into a computer or computer network to steal or delete data.

Hacking is often taken in negative sense but there are many people who hack into the system legally to identify the potential threats in the network. These people are known as ethical hackers. Ethical hacking and Ethical hacker are terms used to describe hacking performed by an individual or company to identify potential threats on a computer or network. An ethical hacker searches for the weak points that could be used by malicious hackers. The organizations use this information to improve the system security, in order to eliminate any potential attacks.

People believe that there is no such thing as an ethical hacker/ethical hacking. Hackers are referred to as computer criminals or cyber criminals. The work done by ethical hacker, may improve the security of any organization. Individuals interested in becoming an ethical hacker can work towards a certification courses offered by various organizations to become a certified ethical hacker (CEH) [13].

4.1 What Constitutes Ethical Hacking

Ethical hackers hack into the system legally and ethically. Ethical hackers detect the threats and loop holes in the company's security system, and protect the company's network and computers from further attack. For hacking to be considered ethical, the hacker must obey the following rules [13]:

- Hackers must get the permission to investigate the network and try to identify the security risks.
- Hackers must respect the privacy of a company or an individual.
- Hackers must close their work and must not leave anything open for someone else to exploit it at later time.
- Hackers should report any security vulnerabilities in a software or hardware, if not already known by the company.

4.2 Reasons for Hacking

With the advance in the computer and the technology, there is a huge threat to the network and the system by the hackers. There are many reasons for which hackers hack the network and systems to attain unauthorized access. Sometimes hackers hack the system to show off that they are capable of hacking the system. The various reasons for hacking are described below [14]:

- **Theft of service:** Every system offers some types of services and if a hacker wants to use those services, they will hack the system. Example of such system is online information network.
- **Take valuable files:** The second reason a hacker may hack into the system is to take the valuable and costly files. Example is credit card numbers. These hackers know that their activities are unlawful and they can get punished.
- **Vengeance and hate:** This is the third reason for hacking. It may cause harm to people.
- **Thrill and excitement:** This is the fourth reason of hacking. Hackers try to access the files and data, to which they are not authorized. This accounts for the vast majority of "true hacking".
- **For knowledge and experiment:** This is the final reason of hacking. Here hackers hack to get new programming knowledge. Hackers learn great deal every time they break into a new type of system.

5. SECURITY BASED ETHICAL ISSUES OF AN ORGANIZATION

The foundation of all secure systems includes moral principles, security practices and the professional etiquettes of employees in the organization. Figure 3 shows issues which an organization has regarding security practices. These issues are discussed below [15]:

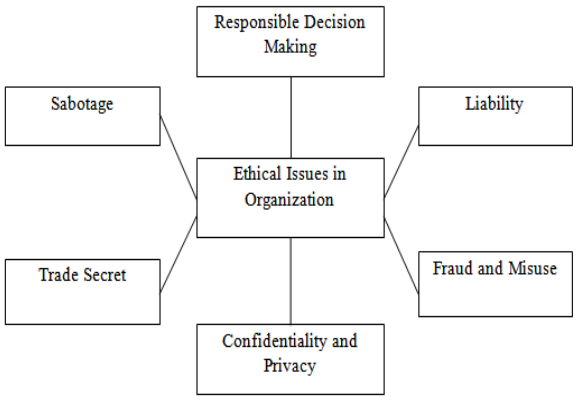

Fig 3: Security Based Ethical Issues In Organization.

- **Ethics and responsible decision making:** For the foundation of security systems, moral principles are needed. People are the part of the solution, but mostly they are the problem creators. An organization may have to deal with many security problems such as responsible decision making, confidentiality, privacy, piracy, fraud

and misuse, liability, trade secrets etc. Employees should be able in making ethical decisions associated with information security.

- **Confidentiality and privacy:** The computer has made invasion to our privacy very easier. Various data are collected and stored in computerized files related to individuals. These files may contain banking information, credit card information, driver license, medical records, organizational fund raising etc. There are various potential threats to privacy which may include improper commercial use of computer data, breach of confidentiality, and release of personal record to government agencies for investigative purposes.
- **Piracy:** It is the unlawful copying, sharing, use etc. of software without the permission of its owner. In an organization pirated software's should be avoided because it violates the basic law of copyright.
- **Fraud and misuse:** Individuals can create a unique environment with the help of computers in which unauthorized activities can occur. Computer related fraud includes the introduction of fraudulent record into a computer system, theft of money by electronic means, theft of financial instruments, theft of services, theft of valuable data etc. Personal information or health information of any individual can be misused.
- **Liability:** Software developers make promises to the users about the nature and quality of the program, these promises can be classified as an express warranty. Thus developers have to be practical about the capabilities, quality, and nature of their software and hardware. Every word they say may be as legally effective as though stated in writing. Thus, to protect against liability, every agreement should be in writing.
- **Patent and copyright law:** Unique and secret aspects of an idea can be protected by a patent. In computer software, complete details of a program by the patent holder are disclosed to allow a skilled programmer to build a program. Copyright law provides a significant tool for protecting computer software, both before and after a security breach. This type of breach could deal with misappropriation of data, computer programs, documentation, or similar material. For this reason, the concept of copyright law must be made familiar to the information security specialist.
- **Trade secrets:** It is a practice, procedure, commercial method or collection of information which is not generally known to others. Economic advantage can be achieved with trade secrets. Trade secret is also known as confidential information. It should be kept secret.
- **Sabotage:** Sabotage is unauthorized use of computer facilities, alteration or destruction of information, data file sabotage and vandalism against a computer system. Computers should be protected from sabotages to avoid any inconvenience.

5.1 Impact of Technology on Privacy of People

As technology increases, it poses a threat on the privacy of people. The impact of the use of technology on the privacy of people demonstrates itself in a variety of areas. These areas are described as below [16]:

- **The electronic monitoring of the people in the workplace:** This is done by CCTV camera. According to justification of companies they use this technology in order to increase the productivity. But it threatens the privacy of the people and technology can lead a feeling of fear or being watched by all the time.
- **Interception and reading of e-mail messages:** It poses an ethical problem related to the private communication of an individual. Companies justify it by saying that they check the e-mail to see resources belong to the company and not to the individual and to check whether employees use the facility for right purpose or not.
- **Merging of databases which contain personal information:** It is also known as data banking. Merging of personal data is done in one central database from different databases. Here the individual is not aware of personal information being integrated into a central database and for what reason or by whom and the information is accurate or not.
- **Hackers and crackers:** They are threat to privacy because they break into the network and computer system and can steal important and personal data. They can even destroy the system.

6. ANALYSIS

There is always an ambiguity that a person is ethical or unethical. Ethics is a range and every unethical action doesn't measure the same on that range. For example, if you told a lie to protect someone's life that would be considered a good ethical choice. Less harm is done by the lie than by telling the truth and putting a life at risk.

Computer security can be achieved by computer ethics. For computers, ethics is used to describe the philosophical principles of right and wrong in relation to the use of computers. By implementing ethics, we can stop the unauthorized access to one's personal data and files. Thus we can prevent people from invading the privacy of other individuals. In various cases people do not follow ethics, the examples are given under:

People use pirated software, CD's, DVD's etc. which is ethically incorrect to use because pirated software are copied and distributed without any authorization.

Let us talk about file sharing. Let us take an example of a person who buys a book and shares it with his/her friends by making a PDF file of that book. Ethically it is not correct to make a PDF file of any book and share PDF with others. It causes loss to the author who has written that book.

When we take the example of the internet, many people claim that internet is a democratic technology. People must use this technology ethically. While chatting on internet people must not fool others by pretending to be someone else and hiding their own identity. Also one must avoid chatting with strangers and shearing personal information with them.

7. CONCLUSION

Above analysis shows that ethics are important in all aspects of life. Ethics is an approach, not a standard set of behaviour. Both ethical and unethical practices co-exist. The common question "is it ethical", has a great significance and must be answerable by every individual. Ethics must be followed and complied to fulfil security objectives in any organization. Security measures are quantifiable but the parameter of ethics is relative to the circumstances and entities involved. As a part

of future work we would like to focus on discrete ethical parameters governing quantifiable security objectives. The discrete ethical variables can be derived by using fuzzy logic, unsupervised learning etc.

8. REFERENCES

[1] "History of ethics", *Wikipedia*, 2016. [Online] https://en.wikipedia.org/wiki/History_of_ethics.

[2] Stallings, W. 2011 Cryptography And Network Security Principles And Security. Pearson Publication.

[3] "Difference Between Ethics and Integrity", *Difference Between*, 2015. [Online] http://www.differencebetween.com/difference-between-ethics-and-vs-integrity/.

[4] "Ethics", *Wikipedia*, 2015. [Online]https://en.wikipedia.org/wiki/Ethics

[5] "Golden Rule", *Wikipedia*, 2016. [Online]https://simple.wikipedia.org/wiki/Golden_Rule.

[6] "Categorical imperative", *Wikipedia*, 2016. [Online]https://en.wikipedia.org/wiki/Categorical_imperative.

[7] "Descartes' rule of change", *Paginas.fe.up.pt*, 2016. [Online] http://paginas.fe.up.pt/~als/mis10e/ch4/descartes.htm.

[8] "Utilitarianism", *Wikipedia*,2016. [Online]https://en.wikipedia.org/wiki/Utilitarianism.

[9] "Risk aversion", *Wikipedia*, 2016. [Online] https://en.wikipedia.org/wiki/Risk_aversion.

[10] Safire, W. 2-14-1993 On Language; "Words Left Out in the cold" New York Times.

[11] "Ten Commandments of Computer Ethics", *Wikipedia*, 2016.[Online] https://en.wikipedia.org/wiki/Ten_Commandments_of_Computer_Ethics.

[12] "Computer Security Ethics and Privacy | WebReference", *Webreference.com*.[Online]http://www.webreference.com/internet/security/index.html.

[13] "What is ethical hacking and an ethical hacker?", *Computerhope.com*.[Online]http://www.computerhope.com/jargon/e/ethihack.htm.

[14] "Internet Security: Ethics / Mateti", *Cecs.wright.edu*, 2016.[Online] http://cecs.wright.edu/~pmateti/InternetSecurity/Lectures/Ethics/.

[15] "03. (III) Ethical Issues", *Niatec.info*, 2016. [Online]http://niatec.info/ViewPage.aspx?id=153.

[16] [Online]http://web.simmons.edu/~chen/nit.NIT'96/96_025_Britz.html.