Abstract

Information security officers, practitioners and academics agree that information security policy in the basis of any organization’s information security. Information security practitioners share and agree the it is rare the information security policy bring out the desirable results. In order to study and analyses this problem, academic have focused on various method to motivate employee toward policy compliance, however, they have not paid much attention on employees’ expectation and how they perceive the information security policy. Also, employees’ satisfaction and awareness of information security policy is critical as it may improve the security level by decreasing the internal threat risks. In this survey, analyzing organization’s employees’ expectation about information security policies based on a framework that is formed regarding internal threat motivation, consequences, security behavior and security countermeasures. Therefore, single case study was adopted in this survey. The study outcome along with the case study findings state that organizations employees’ expectations toward an information security policy should be paid much attention during forming security regulation and even during implementation of information security policy within organizations. The survey conclude that employees’ security behavior is related to their information security background and awareness, as well as, security countermeasures, where if the countermeasures perceived negatively, it may negatively help to increase the risk in term of internal threat. Finally, security countermeasure must be defined before taking negative action towards employees, as well as, information security training should be scheduled regularly within organization and they should be arranged regarding to the organization groups’ professions.

Introduction

Ethics is a field of study that is concerned with distinguishing right from wrong, and good from bad. It analyzes the morality of human behaviors, policies, laws and social structures. Ethicists attempt to justify their moral judgments by reference to ethical principles of theories that attempt to capture our moral intuitions about what is right and wrong. The two theoretical approaches that are most common in ethics are *consequentialism* and *deontology*. Consequentialist approaches assume that actions are wrong to the extent that they have bad consequences, whereas deontological approaches assume that people have moral duties that exist independently of any good or bad consequences that their actions may have. Ethical principles often inform legislation, but it recognized in ethics that legislation cannot function as a substitute for morality. Ethical analysis of security and privacy issues in information technology primarily takes place in *computer ethics* which emerged in the 1980s as a field. Computer ethics analyzes moral responsibilities of computer professionals and computer users and ethical issues in public policy for information technology development and use. It asks such questions as: Is it wrong for corporations to read their employee’s e-mail? Is it morally permissible for computer users to copy copyrighted software? Should people be free to put controversial or pornographic content online without censorship? Ethical issues and questions like these require *moral* or *ethical* *analysis*: analysis in which the moral dilemmas contained in these issues are clarified and solutions are proposed for them. Moral analysis aims to get clear on the facts and values in such cases, and to find a balance between the various values, rights and interests that are at stake and to propose or evaluate policies and courses of action Ethics is an important facet of comprehensive security of information systems. survey in ethics in information security have been also carried outside the information security community. Anyhow, we see that the relationship of hackers and information security personnel has not yet been properly analyzed. Our major argument is that hacking ethics is significantly different from information security ethics, and therefore major difficulties must be solved to establish widely accepted standards for ethical usage on information systems and communication networks. This argument is supported by an extensive analysis and comparison of philosophical and ethical theories. This analysis leads to quite opposite results of the main stream arguments that support the need of common ethical foundation for the security of information systems. A new group and social contract-based security layer shall be added on top of ethical layer. This addition provides with a framework that is feasible within the current technology, supports natural social behavior of human beings, and is iterative enabling forming of larger communities from smaller units. Typically, the hacking community has been arguing for the freedom of information. Security community has been opposing by arguing that system intrusion and hacking, even if no actual harm is caused, is unethical and criminal activity that one should not commit to, even if technically possible. The question rising from this conflict is how can these two groups claim they have a right to tell each other what is ethical and what is not. Recently, the trend appears to be that the ethics approved by the security community is having the law enforcement. Several attempts around the world are made to enforce proper behavior in the information society by juridical methods. From a stereotypic information security point of view hackers are seen as criminals, unaware of the results of their immoral activities making fun out of serious problems. Hacker community, on the other hand, sees information security staff as militants that respecting the freedom of individual and information. These conflicts lead to the fundamental research questions within this paper: Is the ethics-based foundation adequate, and how can it be made more feasible. The scope of this report is limited on philosophical aspects. Comprehensive protection requires several types of technical and non-technical protection measures but technical measures are only considered regarding the feasibility of the proposed approach. Feasibility within current technology is a major requirement for a group-based security model, and as will be shown, our proposal can be enforced by current secure group communication mechanisms. Authors attempt to remain neutral, not arguing for or against any of the ethical systems or opinions analyzed in this report. We also try to keep our personal interpretations of different results neutral and analyses issues objectively. We are combining results of two areas that typically provoke strong emotions: hacking and ethics. Therefore, extensive effort is made to remain objective. Opinions presented in this report do not necessarily represent opinions of authors or organizations they represent but due to objectivity and significance to

Background studies

Confidentiality, integrity, and availability, which is known as for the CIA triad, a model that is designed to guide policies for information security within an organization or a company. The model is also sometimes known as the AIC triad. The elements of the triad are considered the three most crucial components of security.

here, confidentiality provides a Set of rules that provide boundaries to the access to information of an organization or a company, integrity is the assurance that the information is trustworthy and accurate, and availability is a guarantee of reliable access to the information by authorized people.

Confidentiality:

Confidentiality is roughly equivalent to privacy. Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it: Access must be restricted to those authorized to view the data in question. It is common, as well, for data to be categorized according to the amount and type of damage that could be done should it fall into unintended hands. More or less stringent measures can then be implemented according to those categories.

Sometimes safeguarding data confidentiality may involve special training for those privy to such documents. Such training would typically include security risks that could threaten this information. Training can help familiarize authorized people with risk factors and how to guard against them. Further aspects of training can include strong passwords and password-related best practices and information about social engineering methods, to prevent them from bending data-handling rules with good intentions and potentially disastrous results.

A good example of methods used to ensure confidentiality is an account number or routing number when banking online. Data encryption is a common method of ensuring confidentiality. User IDs and passwords constitute a standard procedure; two-factor authentication is becoming the norm. Other options include biometric verification and security tokens, key fobs or soft tokens. In addition, users can take precautions to minimize the number of places where the information appears and the number of times it is actually transmitted to complete a required transaction. Extra measures might be taken in the case of extremely sensitive documents, precautions such as storing only on air gapped computers, disconnected storage devices or, for highly sensitive information, in hard copy form only.

Integrity:

Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle . Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people (for example, in a breach of confidentiality). These measures include file permissions and user access controls. Version control maybe used to prevent erroneous changes or accidental deletion by authorized users becoming a problem. In addition, some means must be in place to detect any changes in data that might occur as a result of non-human-caused events such as an electromagnetic pulse (EMP) or server crash. Some data might include checksums, even cryptographic checksums, for verification of integrity. Backups or redundancies must be available to restore the affected data to its correct state.

Availability:

Availability is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment that is free of software conflicts. It’s also important to keep current with all necessary system upgrades. Providing adequate communication bandwidth and preventing the occurrence of bottlenecks are equally important. Redundancy, failover, RAID even high-availability clusters can mitigate serious consequences when hardware issues do occur. Fast and adaptive disaster recovery is essential for the worst case scenarios; that capacity is reliant on the existence of a comprehensive disaster recovery plan (DRP). Safeguards against data loss or interruptions in connections must include unpredictable events such as natural disasters and fire. To prevent data loss from such occurrences, a backup copy may be stored in a geographically-isolated location, perhaps even in a fireproof, waterproof safe. Extra security equipment or software such as firewalls and proxy servers can guard against downtime and unreachable data due to malicious actions such as denial-of-service (DoS) attacks and network intrusions.

The need for information security in Organization or IT Company

Information is one of the most important organization assets. For an organization, information is valuable and should be appropriately protected. Security is to combine systems, operations and internal controls to ensure integrity and confidentiality of data and operation procedures in an organization. Information security history begins with the history of computer security. It started around year 1980. In 1980, the use of computers has concentrated on computer centers, where the implementation of a computer security focuses on securing physical computing infrastructure that is highly effective organization. Although the openness of the Internet enabled businesses to quickly adopt its technology ecosystem, it also proved to be a great weakness from an information security perspective. The system’s original purpose as a means of collaboration between groups of trusted colleagues is no longer practical because the usage has expanded into millions of frequently anonymous users. Numerous security incidents related to viruses, worms, and other malicious software have occurred since the Morris Worm, which was the first and shut down 10% of the systems on the Internet in 1988. These incidents have become increasingly complex and costly. However, the information security awareness has been increases. Many organizations have implemented the information security to protect their data.

The information security also enables the safe operation of application implemented on the organization’s Information Technology (IT) systems. This is because to protect the data, the organization will applied or install the appropriate software that will secure the data such as antivirus and others protected applications. So, information security is very important in an organization to protect the applications that implemented in organizations and protect the data store in computer as well. Besides protect the data, the application installed also need to be protect because it can contribute to information lost or damages.

Information security will protect the data the organization collects and used. If the information is left unprotected, the information can be accessed by anyone. If the information falls into the wrong hands, it can destroy lives, dropping business and can also be used to do harm. Information security programs will ensure that appropriate information is protected both business and legal requirements by taken steps to protect the organizations data. In addition, taken steps to protect organizations information is a matter of maintaining privacy and will help prevent identity theft.

In an organization, information is important business assets and essential for the business and thus need appropriate protected. This is especially important in a business environment increasingly interconnected, in which information is now exposed to a growing number and a wider variety of threats and vulnerabilities. Cause damage such as malicious code, computer hacking, and denial of service attacks have become more common, more ambitious, and more sophisticated. So, by implemented the information security in an organization, it can protect the technology assets in use at the organization.

In term of protecting the functionality of an organization, both general management and IT management are responsible for implementing information security that protects the organization ability to function. Information is the most important element in organization to do business. Besides that an organization is kept their customers information, so it is crucial for them to protect the information. Without information, the business cannot be run. By secure the information store; it can enable the organization to run business as well. That’s why the information security is important in organizations.

**Ethical & Security Issues in Information System**

Information systems have made many businesses successful today. Some companies such as Google, Facebook, EBay, etc. would not exist without information technology. However, improper use of information technology can create problems for the organization and employees.

Criminals gaining access to credit card information can lead to financial loss to the owners of the cards or financial institute. Using organization information systems i.e. posting inappropriate content on Facebook or Twitter using a company account can lead to lawsuits and loss of business.

This tutorial will address such challenges that are posed by information systems and what can be done to minimize or eliminate the risks.

In this tutorial, you will learn –

[Cyber-crime](https://www.guru99.com/mis-ethical-social-issue.html#1)

[Information system Security](https://www.guru99.com/mis-ethical-social-issue.html#2)

[Information system Ethics](https://www.guru99.com/mis-ethical-social-issue.html#3)

[Information Communication Technology (ICT) policy](https://www.guru99.com/mis-ethical-social-issue.html#4)

Cyber-crime

Cyber-crime refers to the use of information technology to commit crimes. Cyber-crimes can range from simply annoying computer users to huge financial losses and even the loss of human life. The growth of smartphones and other high-end[Mobile](https://www.guru99.com/mobile-testing.html)devices that have access to the internet have also contributed to the growth of cyber-crime.

**Types of cyber-crime**

**Identity theft**

Identity theft occurs when a cyber-criminal impersonates someone else identity to practice malfunction. This is usually done by accessing personal details of someone else. The details used in such crimes include social security numbers, date of birth, credit and debit card numbers, passport numbers, etc.

Once the information has been acquired by the cyber-criminal, it can be used to make purchases online while impersonating himself to be someone else. One of the ways that cyber-criminals use to obtain such personal details is phishing. **Phishing involves creating fake websites that look like legitimate business websites or emails**.

For example, an email that appears to come from YAHOO may ask the user to confirm their personal details including contact numbers and email password. If the user falls for the trick and updates the details and provides the password, the attacker will have access to personal details and the email of the victim.

If the victim uses services such as PayPal, then the attacker can use the account to make purchases online or transfer funds.

Other phishing techniques involve the use of fake Wi-Fi hotspots that look like legitimate ones. This is common in public places such as restaurants and airports. If an unsuspecting user logons into the network, then cyber-crimes may try to gain access to sensitive information such as usernames, passwords, credit card numbers, etc.

According to the US Department of Justice, a former state department employee used email phishing to gain access to email and social media accounts of hundreds of women and accessed explicit photos. He was able to use the photos to extort the women and threatened to make the photos public if they did not give in to his demands.

**Copyright infringement**

Piracy is one of the biggest problems with digital products. Websites such as the pirate bay are used to distribute copyrighted materials such as audio, video, software, etc. Copyright infringement refers to the unauthorized use of copyrighted materials.

Fast internet access and reducing costs of storage have also contributed to the growth of copyright infringement crimes.

**Click fraud**

Advertising companies such as Google AdSense offer pay per click advertising services. Click fraud occurs when a person clicks such a link with no intention of knowing more about the click but to make more money. This can also be accomplished by using automated software that makes the clicks.

**Advance Fee Fraud**

An email is sent to the target victim that promises them a lot of money in favor of helping them to claim their inheritance money.

In such cases, the criminal usually pretends to be a close relative of a very rich well-known person who died. He/she claims to have inherited the wealth of the late rich person and needs help to claim the inheritance. He/she will ask for financial assistance and promise to reward later. If the victim sends the money to the scammer, the scammer vanishes and the victim loses the money.

**Hacking**

Hacking is used to by-pass security controls to gain unauthorized access to a system. Once the attacker has gained access to the system, they can do whatever they want. Some of the common activities done when system is hacked are;

Install programs that allow the attackers to spy on the user or control their system remotely

Deface websites

Steal sensitive information. This can be done using techniques such as[SQL](https://www.guru99.com/sql.html)Injection, exploiting vulnerabilities in the database software to gain access, social engineering techniques that trick users into submitting ids and passwords, etc.

**Computer virus**

Viruses are unauthorized programs that can annoy users, steal sensitive data or be used to control equipment that is controlled by computers.

Information system Security

MIS security refers to measures put in place to protect information system resources from unauthorized access or being compromised. Security vulnerabilities are weaknesses in a computer system, software, or hardware that can be exploited by the attacker to gain unauthorized access or compromise a system.

People as part of the information system components can also be exploited using social engineering techniques. The goal of social engineering is to gain the trust of the users of the system.

Let's now look at some of the threats that information system face and what can be done to eliminate or minimize the damage if the threat were to materialize.

**Computer viruses** – these are malicious programs as described in the above section. The threats posed by viruses can be eliminated or the impact minimized by using Anti-Virus software and following laid down security best practices of an organization.

**Unauthorized access** – the standard convention is to use a combination of a username and a password. Hackers have learnt how to circumvent these controls if the user does not follow security best practices. Most organizations have added the use of mobile devices such as phones to provide an extra layer of security.

Let's take Gmail as an example, if Google is suspicious of the login on an account, they will ask the person about to login to confirm their identity using their android powered mobile devices or send an SMS with a PIN number which should supplement the username and password.

If the company does not have enough resources to implement extra security like Google, they can use other techniques. These techniques can include asking questions to users during signup such as what town they grew up in, the name of their first pet, etc. If the person provides accurate answers to these question, access is granted into the system.

**Data loss** – if the data center caught fire or was flooded, the hardware with the data can be damaged, and the data on it will be lost. As a standard security best practice, most organizations keep backups of the data at remote places. The backups are made periodically and are usually put in more than one remote area.

Biometric Identification – this is now becoming very common especially with mobile devices such as smartphones. The phone can record the user fingerprint and use it for authentication purposes. This makes it harder for attackers to gain unauthorized access to the mobile device. Such technology can also be used to stop unauthorized people from getting access to your devices.

Information system Ethics

Ethics refers to rules of right and wrong that people use to make choices to guide their behaviors. Ethics in MIS seek to protect and safeguard individuals and society by using information systems responsibly. Most professions usually have defined a code of ethics or code of conduct guidelines that all professionals affiliated with the profession must adhere to.

In a nutshell, a code of ethics makes individuals acting on their free will responsible and accountable for their actions. An example of a Code of Ethics for MIS professionals can be found on the British Computer Society (BCS) website.

Information Communication Technology (ICT) policy

An ICT policy is a set of guidelines that defines how an organization should use information technology and information systems responsibly. ICT policies usually include guidelines on;

Purchase and usage of hardware equipment and how to safely dispose them

Use of licensed software only and ensuring that all software is up to date with latest patches for security reasons

Rules on how to create passwords (complexity enforcement), changing passwords, etc.

Acceptable use of information technology and information systems

Training of all users involved in using ICT and MIS

Perspective of information security in Bangladeshi organization