International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 1 Issue 2 July 2011

SECURITY AND ETHICAL ISSUES IN IT: AN ORGANIZATION'S PERSPECTIVE

Devendra Kumar Tiwary
Assistant Professor, Department of Computer Application,*
Technical Education & Research Institute,
Post-Graduate College, Ravindrapuri, Ghazipur,
Uttar Pradesh (INDIA)

ABSTRACT

Information Technology is changing the face of contemporary World. The IT has not only connected the World at one single platform but it is also helping in the integration of various traditional societies into modern societies. Information systems raise new and often-perplexing security and ethical problems. This is truer today than ever because of the challenges posed by the Internet and electronic commerce to the protection of privacy and intellectual property. Information technology has raised new possibilities for behavior for which laws and rules of acceptable conduct have not yet been developed. Information technology is introducing changes that create new security and ethical issues for societies to debate and resolve. Increasing computing power, storage, and networking capabilities—including the Internet—can expand the reach of individual and organizational actions and magnify their impacts. The ease and anonymity with which information can be communicated, copied, and manipulated in online environments are challenging traditional rules of right and wrong behavior. Ethical issues confront individuals who must choose a course of action, often in a situation in which two or more ethical principles are in conflict. This paper argues that we must reconsider our approach to information security from the ground up if we are to deal effectively with the problem of information risk.

Keywords: Challenges, Ethics, Information System, Information Technology, Security.

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 1 Issue 2 July 2011

Introduction

Security is a broad topic and covers a multitude of sins. In its simplest from, it is concerned with making sure that nosy people can not read, or worse yet, modify messages intended for other recipients. It is concerned with people trying to access remote services that they are not authorized to use. Most security problems are intentionally caused by malicious people trying to gain some benefit or harm someone. Student have fun snooping on people's email, hacker hacks to test out someone's security system or steal information, businessman causes breach in security to discover a competitor's strategic marketing plan, an ex-employee leaks information to get revenge for being fired, a terrorist to steal germ warfare secrets. These all unauthorized access to information system causes serious security problems.

Data security is a broad category of activities that covers all aspects of protecting the integrity of a computer or computer network. Under its most liberal interpretation, data security involves protecting a computer from external threats (from individuals outside the organization), internal threats (from individuals within the organization) and from threats to hardware as well as to software. In this interpretation, disaster recovery can be considered a part of data security as information managers seek to protect data from natural disasters and manmade attacks.

Organizations can improve their security by simply observing fundamental strategies such as using only licensed copies of software which are unlikely to have viruses installed on them and by limiting access to computers and files on those computers. Just as physical files have limited access points, so data files should also be limited to those individuals who have a business reason for viewing the files. Passwords and access codes provide rudimentary security at this level, and will prevent access by the merely curious. Information security is important in proportion to an organization's dependence on information technology. When an organization's information is exposed to risk, the use of information security technology, however, deals with only a small fraction of the problem of information risk. In fact, the evidence increasingly suggests that information security technology does not reduce information risk very effectively.

Ethics refers to the principles of right and wrong that individual, acting as free moral agents; use to make choices to guide their behaviors. Information systems raise new ethical questions for both individuals and societies because they create opportunities for intense social change, and thus threaten existing distributions of power, money, rights, and obligations. Like other technologies, such as steam engines, electricity, the telephone, and the radio, information technology can be used to achieve social progress, but it can also be

used to commit crimes and threaten cherished social values. The development of information technology will produce benefits for many and costs for others.

Computer Ethics is a branch of practical philosophy which deals with how computing professionals should make decisions regarding professional and social conduct. Margaret Anne Pierce, a professor in the Department of Mathematics and Computers at Georgia Southern University has categorized the ethical decisions related to computer technology and usage into 3 primary influences:

- ✓ The individual's own personal code.
- ✓ Any informal code of ethical behavior that exists in the work place.
- ✓ Exposure to formal codes of ethics.

Physicians, attorneys and other professionals whose job duties affect others' lives usually receive, as part of their formal training, courses that address ethical issues common to their professions. IT security personnel often have access to much confidential data and knowledge about individuals' and companies' networks and systems that give them a great deal of power. That power can be abused, either deliberately or inadvertently. But there are no standardized training requirements for hanging out your shingle as an IT security consultant or in-house security specialist. Associations and organizations for IT pros are beginning to address the ethical side of the job, but again, there is no requirement for IT security personnel to belong to those organizations. The education and training of IT professionals, including security specialists, usually focuses on technical knowledge and skills. You learn *how* to perform tasks, but with little consideration of how those abilities can be misused. In fact, many IT professionals approach their work with a hacker's perspective: whatever you *can* do, you're entitled to do.

Information systems raise new and often-perplexing security an ethical problems. This is truer today than ever because of the challenges posed by the Internet and electronic commerce to the protection of privacy and intellectual property. Other security and ethical issues raised by widespread use of information systems include establishing accountability for the consequences of information systems, setting standards to safeguard system quality that protect the safety of individuals and society, and preserving values and institutions considered essential to the quality of life in an information society. If organization running a large business, it will be confronting these issues, and organization need to know how to deal with them.

Security Management: A closer look

Information Security can only be managed properly if, on a macro level, an internationally accepted reference framework (code of practice) is used, and if on a micro level, physical measurements can be made. All this must be accompanied by an international information

security certificate, and a comprehensive corporate information security culture. There are plenty of tools to enforce security in information system. Information being a vital resource for organization must be kept secure from unauthorized access. Security tools minimize errors, fraud, and losses in the e-business systems that interconnect businesses with their customers, suppliers, and other stakeholders.

Encrypted passwords, messages, files, and other data is transmitted in scrambled form and unscrambled for authorized users. It involves using special mathematical algorithms to transform digital data in scrambled code. Most widely used method uses a pair of public and private keys unique to each individual. Firewalls serve as a “gatekeeper” system that protects a company’s intranets and other computer networks from intrusion. Firewalls provide a filter and safe transfer point. It prevents malicious agents by screening all network traffic for proper passwords or other security codes.

The development of information security over the last 40 to 50 years can probably be described in many ways. One way, which divides the development into three waves, and which does seem to provide a good representation of the development of the field. The ‘First Wave’, up to about the early eighties, can be seen as the ‘Technical Wave’, mainly characterized by a very technical approach to information security. The ‘Second Wave’, from about early eighties to middle nineties, can be seen as the ‘Management Wave’, characterized by a growing management realization of and involvement with the importance of information security, supplementing the Technical Wave. These two waves were well established by the end of the nineties. From the last few years of the nineties, a third wave started. This ‘Third Wave’ we call the ‘Institutional Wave’. This wave is characterized by aspects like best practices and codes of practice for information security management, international information security certification, cultivating information security as a corporate culture, and dynamic and continuous information security management.

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 1 Issue 2 July 2011

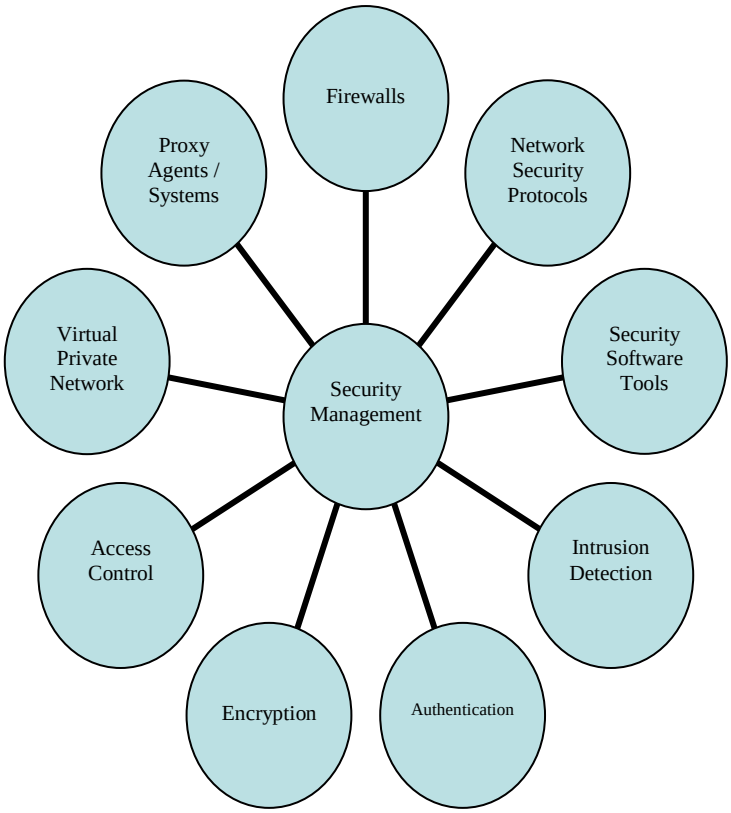

Figure 1: Security Management Tools

Where information risk is well enough understood and at least in broad terms stable, information security starts with policies. These policies describe "'who should be allowed to do what" to sensitive information. Once an information security policy has been defined, the next task is to enforce the policy. To do this, the business deploys a mix of processes and technical mechanisms. These processes and mechanisms fall into four categories:

- Protection measures (both processes and technical mechanisms) aim to prevent adverse events from occurring.
- Detection measures alert the business when adverse events occur.
- Response measures deal with the consequences of adverse events and return the business to a safe condition after an event has been dealt with.

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 1 Issue 2 July 2011

- Assurance measures Validate the effectiveness and proper operation of protection, detection, and response measures.

The final information security task is an audit to determine the effectiveness of the measures taken to protect information against risk, we say "final" but, obviously, the job of information risk management is never done. The policy definition, protection, and audit tasks are performed over and over again, and the lessons learned each time through the cycle are applied during the next cycle.

Ethical Challenges

Ethical issues in information systems have been given new urgency by the rise of the Internet and electronic commerce. Internet and digital firm technologies make it easier than ever to assemble, integrate, and distribute information, unleashing new concerns about the appropriate use of customer information, the protection of personal privacy, and the protection of intellectual property. Insiders with special knowledge can “fool” information systems by submitting phony records, and diverting cash, on a scale unimaginable in the pre-computer era. Other pressing ethical issues raised by information systems include establishing accountability for the consequences of information systems, setting standards to safeguard system quality that protects the safety of the individual and society, and preserving values and institutions considered essential to the quality of life in an information society. When using information systems, it is essential to ask, “What is the ethical and socially responsible course of action?”

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 1 Issue 2 July 2011

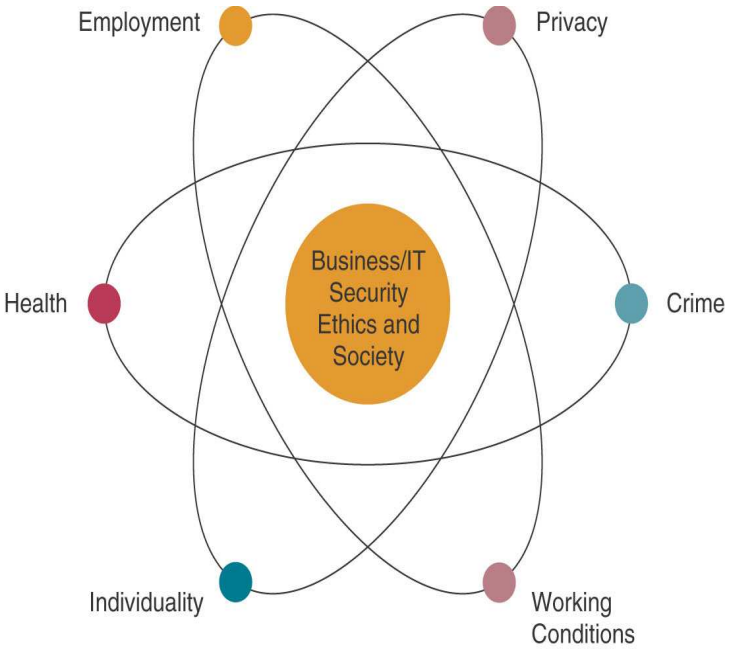

Figure 2: Ethical Responsibilities

Issues of IT Ethics have recently become immensely more complex. The capacity to place material on the World Wide Web has been acquired by a very large number of people. As evolving software has gently hidden the complexities and frustrations that were involved in writing HTML, more and more web sites are being created by people with a relatively modest amount of computer literacy. At the same time, once the initial reluctance to use the Internet and the World Wide Web for commercial purposes had been overcome, sites devoted to doing business on the Internet mushroomed and e-commerce became a term permanently to be considered part of common usage. The assimilation of new technology is almost never smooth. As the Internet begins to grow out of its abbreviated infancy, a multitude of new issues surface continually, and a large proportion of these issues remain unresolved. Many of these issues contain strong ethics content. As the ability to reach millions of people instantly and simultaneously has passed into the hands of the average person, the rapid emergence of thorny ethical issues is likely to continue unabated.

An organization has to cope with major types of ethical issues. These are: Privacy and personal information, Freedom of speech in cyberspace, Intellectual property and Cyber crime. Privacy is the claim of individuals to be left alone, free from surveillance or interference from other individuals or organizations, including the state. Claims to privacy are

also involved at the workplace: Millions of employees are subject to electronic and other forms of high-tech surveillance. Information technology and systems threaten individual claims to privacy by making the invasion of privacy cheap, profitable, and effective. Internet technology has posed new challenges for the protection of individual privacy. Information sent over this vast network of networks may pass through many different computer systems before it reaches its final destination. Each of these systems is capable of monitoring, capturing, and storing communications that pass through it. Within the organization personal privacy is violated. Below are some facts how individual privacy is broken at workplace [1].

- 62% of employers monitor employees' email and Internet use.
- 68% cite legal liability as the primary reason to monitor.
- 87% of companies that monitor have a written email Policy,
- 83.1% an Internet Policy,
- 68% a Software Policy.
- 51% of employers have disciplined or terminated employees for violating ePolicy.
- 35% of organizations have email retention & deletion policies in place.
- 10% of companies have been ordered by courts to turn over employee email related to workplace lawsuits.
- 8.3% of organizations have battled sexual harassment and/or sexual discrimination claims stemming from employee e-mail and/or Internet use.

Much is discussed about privacy laws in developed economies such as the US, EU, Japan, Canada, and Australia. However, not many studies have focused on privacy laws that are evolving in emerging economies such as India. As the economy becomes global and companies resort to global outsourcing, much of the data of clients, customers and common citizens are slowly being dispersed around the world for processing, analyzing and simple storage. Therefore, developing countries that handle such data are no longer exempt from the privacy concerns associated with them.

---

[1]. Source: The 2001 Electronic Policies & Practices Survey from The American Management Association, US News & World Report, and The ePolicy Institute.

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 1 Issue 2 July 2011

Computer crime refers to the unauthorized use, access, modification, and destruction of hardware, software, data, or network resources, unauthorized release of information, unauthorized copying of software. There are no precise, reliable statistics on the amount of computer crime and the economic loss to victims, partly because many of these crimes are apparently not detected by victims, many of these crimes are never reported to authorities, and partly because the losses are often difficult to calculate. Nevertheless, there is a consensus among both law enforcement personnel and computer scientists who specialize in security that both the number of computer crime incidents and the sophistication of computer criminals are increasing rapidly. Experts in computer security, who are *not* attorneys, speak of "information warfare". While such "information warfare" is just another name for computer crime, the word "warfare" does fairly denote the amount of damage inflicted on society.

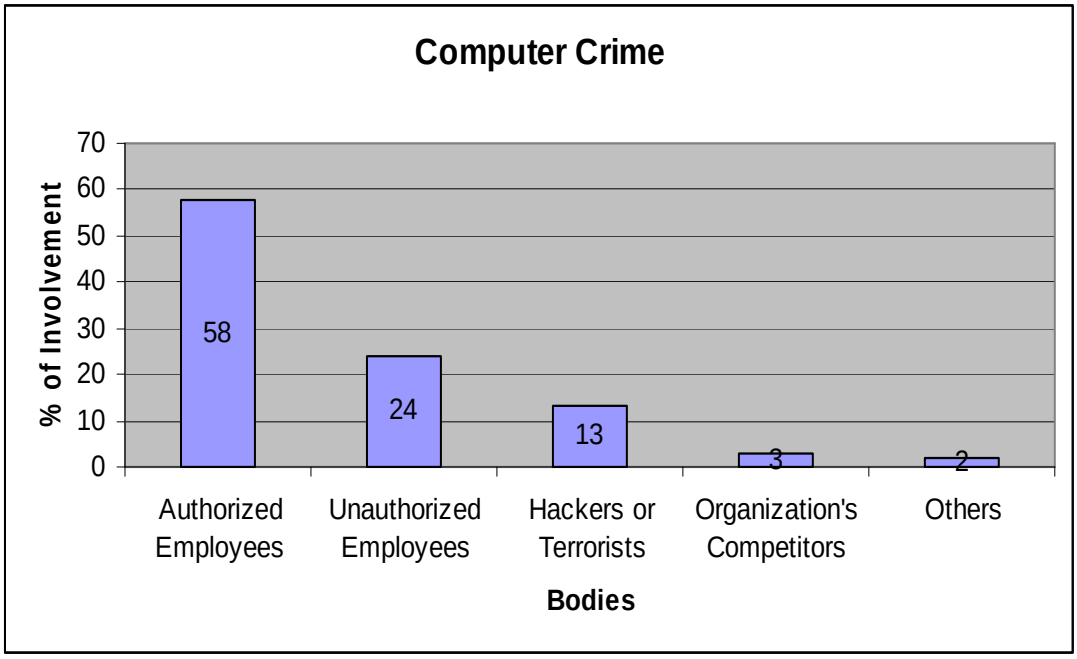

Figure 3: Computer crimes by various bodies

Suggestive Measures

Using IT in business activities enhances productivity of all components of the organization. But these enhancements are not free of cost. Use of IT in business causes information risks. Therefore a trade off between rewards and risks exist. The organization must ensure the

some rules to preserve their information, the privacy of working staff and to reduce the risks of computer crimes.

1. Whether to use IT tools and technologies in organization is purely depends on the need of organization. With the advance of technology, problems are inevitable. One major issue emerging is the security of sensitive information. Technologies such as cloud computing, social networking and wireless applications allow companies to streamline operations. Cloud computing allows businesses to move to a more efficient information technology (IT) model. Businesses save money on IT, energy and real estate costs due to the centralization of data on servers. Social networking increases customer rapport, allowing for potentially greater profits and increasing customer loyalty. Using these tools and technologies also impose additional cost to company. Many organizations introduce latest technologies for their work without requirements causing serious problems of security risks. Therefore don't be the crowed follower.

2. Use of licensed and authentic software will reduce security risks. The potential for modern business software to take a business into the future cannot be underestimated, today's customers require, and expect service of the highest quality. If your business does not supply such a service, it is about time it did. Full integration of departments is fundamental to ensuring exceptional service is provided to customers. After all they are the most important asset any business can possess. Pirated copy of software cost less but it liable to failure in future. It is also a criminal offence and subject to legal proceedings.

3. Standard and reliable data storage media, backup and recovery technologies provide a cornerstone of data protection strategies that help organizations meet their requirements for data availability and accessibility. Storing, restoring, and recovering data are key storage management operational activities surrounding one of the most important business assets: corporate data. Data centers can use redundant components and fault tolerance technologies to replicate crucial data to ensure high availability. However, these technologies alone cannot solve issues caused by data corruption or deletion, which can occur due to application bugs, viruses, security breaches, or user errors. There may also be a requirement for retaining information in an archival form, such as for industry or legal auditing reasons; this requirement may extend to transactional data, documents, and collaborative information such as e-mail. Therefore, it is necessary to have a data protection strategy that includes a comprehensive backup and recovery scheme to protect data from any kind of unplanned outage or disaster, or to meet industry requirements for data retention.

4. Centralized data storage reduces the problems of information loss or theft. The centralized data is secured behind multiple layers of firewalls and intrusion detection

systems and managed by Information Technology (IT) professionals whose profession it is to the data safe. In the Centralized Data model, responsibility for the integrity and safety of the data is no longer organization alone to bear, but is shared with the company hosting the data. It thus becomes in the best interest of that host to ensure data is kept safe. This means an investment in the infrastructure (servers, disk drives, database software, firewalls, backups, redundancy, etc.) that is exponentially safer (and more expensive!) than anything that can be done locally.

5. Parallel run strategy minimizes system failure. Parallel run is a method for transferring between an old system to a target system in an organization. In order to reduce risk, the old and new system run simultaneously for some period of time after which, if the criteria for the new system are met, the old system is disabled. The process requires careful planning and control and a significant investment in labor hours. In this way information can be retrieved even after failure of old system.

6. The employees should be enriched with the code of ethics by internal training. Ethics training programs help in building strong teams and foster professionalism in the workplace, thus increasing work productivity. Due to the prevalence of ethical culture in the organization, the quality of goods and services provided by the company is not compromised. Hence, ethics training helps in quality management. A company whose employees are known for strong business ethics has a strong public image. This results in increased sales and profits, as the people trust their products and services more than those of any other company.

7. White Hat Hackers are beneficial. They can discover loop holes in security system. White hat hackers usually play in the field of black hat hacking, but they do not deface or steal information. Instead, they will notify the company that the corporate network has been breached and consult them in how to fix the holes. Hiring a white hat hacker is beneficial for the company, because the hacker has a sense of protection for innocent users. A white hat hacker still knows the issues faced with security, and some of them partake in the security "wars" that exist on various servers. These security consultants play at night, but they can detect and protect a business from theft during the day.

8. Technology is not the solution of all business problems. An incorrect decision is often the result of starting with the technology rather than the business process. A decade ago, technology was seen as the solution to all business problems; i.e., just get the right system and your troubles are over. Today, however, technology is properly viewed as the implementation of the solution. Technology is an essential component of the solution, but only a component. An effective solution must start with the business processes that generate and use the information that is managed and stored by the information

system. The business process must drive the choice or design of technology, not vice versa. This may seem an obvious statement, but it is one unfortunately overlooked by too many companies.

Conclusion

It is a myth that black hat hackers cause most security breaches but in reality, 80% of data loss is caused by insiders. To design a security solution that truly protects data, organization must understand the security requirements relevant to its business process, and the scope of current threats to data.

A business, using IT tools heavily, depends on providing customers, partners, and employees with access to information, in a way that is controlled and secure. Managing such types of business security is a multifaceted challenge and requires the coordination of business policy and practice with appropriate technology. In addition to deploying standards bases, flexible and interoperable systems, the technology must provide assurance of the security provided in the products. As technology matures and secure information systems are deployed, companies will be better positioned to manage the risks associated with disintermediation of data access. Through this process businesses will enhance their competitive edge while also working to protect critical business infrastructures from malefactors like hackers, disgruntled employees, criminals and corporate spies.

It is probably not possible to develop comprehensive ethical guidelines to cover every possible situation of IT misuse in inside or outside the organization. It is possible, however, to realize the pervasiveness and the magnitude of the problem. It is also possible to develop ethical guidelines on an ongoing basis to keep pace with changes in the issues. Codes of ethics and professional conduct vary from one professional organization to the next and are incomplete or obsolete.

References

[1] Anthony D. Miyazaki and Ana Fernandez, “Consumer Perceptions of Privacy and Security Risks for Online Shopping”, 2006.

[2] ACM Code of Ethics and Professional Conduct (1992). Communications of the ACM, 35(5), 94-99.

[3] Beynon-Davies P., Business Information Systems. Palgrave, Basingstoke, 2009.

---

[4] Bynum, Terrell Ward, A very short history of computer ethics, Southern Connecticut State University, 2008.

[5] Computer Security Institute and US FBI, Computer Security Issues & Trends, CSI 2000.

[6] Forester, T. and Morrison, P. Computer Ethics, MIT Press, Cambridge, Mass., 1990.

[7] Harrington, S.J., The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions, MIS Quarterly, 20, 3 (1996), 257–278.

[8] http://www.acm.org/about/code-of-ethics.

[9] IEEE code of ethics. http://ieee.org.

[10] ISO/IEC 17799 Code of practice for Information Security Management, International Organization for Standardization.

[11] Kling, R., Computer abuse and computer crime as organizational activities, Computers and Law J. 2 (Spring 1980).

[12] Margaret, A, & Henry, J., Journal of business ethics, Computer Ethics: The Role of Personal, Informal, and Formal Codes, 15(4), 425.

[13] Mason, R.O., Four ethical issues of the information age*, MIS* Quarterly, 10, 1 (1986), *5–12.*

[14] O'Brien, J A., Introduction to information systems: essentials for the e-business enterprise, McGraw-Hill, Boston, MA, 2003.

[15] Parker, D.B., Swope S., & Baker, B.N., Ethical Conflicts in Information and Computer Science, Technology and Business, 1990*,* Wellesley, MA: QED Information Sciences.

[16] Praveen Dalal, ICT Trends in India, 2006

[17] Wood, W.A., Computer Ethics and Years of Computer Use. Journal of Computer Information Systems, 23- 27, 1993