International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 2 –NOVEMBER 2014.

Computer Ethics & Professional Responsibility to Provide Security of Data in the Workplace

[1]Bharathi Devi Patnala and [2]Shamim

[1]HOD, Department of M.C.A., K.B.N. College, Vijayawada

[2]HOD, Department of M.Sc. (CS), K.B.N. College, Vijayawada

Abstract— Computer ethics is a new branch of ethics that is growing and changing rapidly as computer technology also grows and develops. The term "computer ethics" is open to interpretations both broad and narrow. On the other hand, it is possible to construe computer ethics in a very broad way to include, as well, standards of professional practice, codes of conduct, aspects of computer law, public policy, and corporate ethics. In the industrialized nations of the world, the "information revolution" already has significantly altered many aspects of life in banking and commerce, work and employment, medical care, national defence, transportation and entertainment. Consequently, information technology has begun to affect (in both good and bad ways) community life, family life, human relationships, education, freedom, democracy, and so on (to name a few examples). Computer ethics in the broadest sense can be understood as that branch of applied ethics which studies and analyses such social and ethical impacts of information technology. In recent years, this robust new field has led to new university courses, conferences, workshops, professional organizations, curriculum materials, books, articles, journals, and research centres. And in the age of the world-wide-web, computer ethics is quickly being transformed into "global information ethics".

Keywords: computer ethics, professional ethics, ethical commandments

I. INTRODUCTION

Ethics is a set of moral principles that govern the behaviour of a group or individual. Therefore, computer ethics is set of moral principles that regulate the use of computers. Some common issues of computer ethics include intellectual property rights (such as copyrighted electronic content), privacy concerns, and how computers affect society.

For example, while it is easy to duplicate copyrighted electronic (or digital) content, computer ethics would suggest that it is wrong to do so without the author's approval. And while it may be possible to access someone's personal information on a computer system, computer ethics would advise that such an action is unethical.

As technology advances, computers continue to have a greater impact on society. Therefore, computer ethics promotes the discussion of how much influence computers should have in areas such as artificial intelligence and human communication. As the world of computers evolves, computer ethics continues to create ethical standards that address new issues raised by new technologies.

II. COMPUTER ETHICS IN THE WORKPLACE

Computer ethics refers to the ways in which ethical traditions and norms are tested, applied, stretched, negotiated, and broken in the realm of computer technology. As computers brought about dramatically enhanced power of communication and data manipulation, new ethical questions and controversies were forced to the forefront of contemporary ethics debates. While ethics is concerned with codes of behaviour, the arena of computer technology has created many uncertainties that make the establishment of such clear codes an often daunting task.

The more dramatic abuses of computer technology, such as major Internet hackings of company Web sites and online theft of credit card numbers, achieve a high profile. While there are few uncertainties about such cases, these are only the most visible examples of far more prevalent phenomena. Most cases are more subtle, frequent, and tied to the everyday workings of ordinary, law-abiding citizens. There are few clear rules to govern ethical computer behaviour, and novel situations arise with great frequency, which can prove dangerous when these fields and practices are mixed with business and sensitive information.

The sheer scope of computer usage, spanning nearly every part of daily life and work, from medical records and communications to payment schedules and national defence systems, makes the untangling of ethical considerations all the more important, as unchecked ethical violations in one area can have severe repercussions throughout a wider system. On the personal level, individuals may run into ethical difficulties in considering what other activities they are facilitating by

performing their particular functions via computer. Unfortunately, the speed of computer innovation has usually far outpaced the development of ethical norms to guide the application of new technologies.

The sheer volume of data available to individuals and organizations heightens the concern over computer ethics. The competitive nature of the economy provides an incentive to beat competitors to certain advantageous practices so as to capitalize on those advantages. The trick, then, is for organizations to devise ethical principles that allow for the greatest level of innovation and competitive strategy while remaining within the bounds of acceptable societal ethics, thereby maintaining the stability of the system from which they hope to benefit. Likewise, businesses need to coordinate codes of ethics to avoid having their own information systems compromised and putting themselves at a disadvantage.

Regarding the Internet itself, the ethical conundrum centres on several basic questions. Will this medium have negative effects on society? What preventive measures can and should be taken to protect against these negative effects? In what ways will these preventive measures give rise to even more ethical considerations? Ultimately, how does society balance potential benefits with potentially damaging effects?

Information technology and computer professionals began seriously considering the long-term effects of computer ethics in the late 1980s and early 1990s. They recognized the need to organize professionally through such bodies as the Association for Computing Machinery and the Institute of Electrical and Electronics Engineers to devise professional codes of conduct. However, the increasing proliferation of powerful computers in the hands of non -professionals widens the scope of potential problems.

Public interest groups such as the Computer Ethics Institute have made attempts to draw out basic guidelines for ethical computer behaviour applicable throughout society. In that spirit, the institute formulated the "Ten Commandments of Computer Ethics," a list of basic dos and don'ts for computer use. Several professional associations have attempted to devise computer ethics codes. The code devised by the Association for Computing Machinery, for instance, included specific instructions that it is "the responsibility of professionals to maintain the privacy and integrity of data describing individuals," and that clear definitions for the retention and storage of such information and the enforcement thereof must be implemented for the protection of individual privacy.

III. COMPUTER CRIME

In this era of computer "viruses" and international spying by "hackers" who are thousands of miles away, it is clear that computer security is a topic of concern in the field of Computer Ethics. The problem is not so much the physical security of the hardware (protecting it from theft, fire, flood, etc.), but rather "logical security", which Spafford, Heaphy and Ferbrache [Spafford, et al, 1989] divide into five aspects:

Privacy and confidentiality

Integrity -- assuring that data and programs are not modified without proper authority

Unimpaired service

Consistency -- ensuring that the data and behaviour we see today will be the same tomorrow

Controlling access to resources

Malicious kinds of software, or "programmed threats", provide a significant challenge to computer security. These include "viruses", which cannot run on their own, but rather are inserted into other computer programs; "worms" which can move from machine to machine across networks, and may have parts of themselves running on different machines; "Trojan horses" which appear to be one sort of program, but actually are doing damage behind the scenes; "logic bombs" which check for particular conditions and then execute when those conditions arise; and "bacteria" or "rabbits" which multiply rapidly and fill up the computer's memory. Computer crimes, such as embezzlement or planting of logic bombs, are normally committed by trusted personnel who have permission to use the computer system. Computer security, therefore, must also be concerned with the actions of trusted computer users. Another major risk to computer security is the so-called "hacker" who breaks into someone's computer system without permission. Some hackers intentionally steal data or commit vandalism, while others merely "explore" the system to see how it works and what files it contains. These "explorers" often claim to be benevolent defenders of freedom and fighters against rip-offs by major corporations or spying by government agents. These self-appointed vigilantes of cyberspace say they do no harm, and claim to be helpful to society by exposing security risks. However every act of hacking is harmful, because any known successful penetration of a computer system requires the owner to thoroughly check for damaged or lost data and programs. Even if the hacker did indeed make no changes, the computer's owner must run through a costly and time-consuming investigation of the compromised system.

IV. PRIVACY AND ANANOMITY

One of the earliest computer ethics topics to arouse public interest was privacy. For example, in the mid-1960s the American government already had created large databases of information about private citizens (census data, tax records, military service records, welfare records, and so on). In the US Congress, bills were introduced to assign a personal identification number to every citizen and then gather all the government's data about each citizen under the corresponding ID number. A public outcry about "big-brother government" caused Congress to scrap this plan and led the US President to appoint committees to recommend privacy legislation. In the early 1970s, major computer privacy laws were passed in the USA. Ever since then, computer-threatened privacy has remained as a topic of public concern. The ease and efficiency with which computers and computer networks can be used to gather, store, search, compare, retrieve and share personal information make computer technology especially threatening to anyone who wishes to keep various kinds of "sensitive" information (e.g., medical records) out of the public domain or out of the hands of those who are perceived as potential threats. During the past decade, commercialization and rapid growth of the internet; the rise of the world-wide-web; increasing "user-friendliness" and processing power of computers; and decreasing costs of computer technology have led to new privacy issues, such as data-mining, data matching, recording of "click trails" on the web, and so on [see Tavani, 1999].

The variety of privacy-related issues generated by computer technology has led philosophers and other thinkers to re-examine the concept of privacy itself. Since the mid-1960s, for example, a number of scholars have elaborated a theory of privacy defined as "control over personal information" (see, for example, [Westin, 1967], [Miller, 1971], [Fried, 1984] and [Elgesem, 1996]). On the other hand, philosophers Moor and Tavani have argued that control of personal information is insufficient to establish or protect privacy, and "the concept of privacy itself is best defined in terms of restricted access, not control" [Tavani and Moor, 2001] (see also [Moor, 1997]). In addition, Nissenbaum has argued that there is even a sense of privacy in public spaces, or circumstances "other than the intimate." An adequate definition of privacy, therefore, must take account of "privacy in public" [Nissenbaum, 1998]. As computer technology rapidly advances -- creating ever new possibilities for compiling, storing, accessing and analyzing information -- philosophical debates about the meaning of "privacy" will likely continue (see also [Introna, 1997]).

For example, if someone is using the internet to obtain medical or psychological counselling, or to discuss sensitive topics (for example, AIDS, abortion, gay rights, venereal disease, and political dissent), anonymity can afford protection similar to that of privacy. Similarly, both anonymity and privacy on the internet can be helpful in preserving human values such as security, mental health, self-fulfilment and peace of mind. Unfortunately, privacy and anonymity also can be exploited to facilitate unwanted and undesirable computer-aided activities in cyberspace, such as money laundering, drug trading, terrorism, or preying upon the vulnerable (see [Marx, 2001] and [Nissenbaum, 1999]).

V. PROFESSIONAL RESPONSIBILITY

Computer professionals have specialized knowledge and often have positions with authority and respect in the community. For this reason, they are able to have a significant impact upon the world, including many of the things that people value. Along with such power to change the world comes the duty to exercise that power responsibly [Gotterbarn, 2001]. Computer professionals find themselves in a variety of professional relationships with other people [Johnson, 1994], including:

Employer	--	Employee
Client	--	Professional
Professional	--	Professional
Society	--	Professional

These relationships involve a diversity of interests, and sometimes these interests can come into conflict with each other. Responsible computer professionals, therefore, will be aware of possible conflicts of interest and try to avoid them.

In addition, both the ACM and IEEE have adopted Codes of Ethics for their members. The most recent ACM Code (1992), for example, includes "general moral imperatives", such as "avoid harm to others" and "be honest and trustworthy". And also included are "more specific professional responsibilities" like "acquire and maintain professional competence" and "know and respect existing laws pertaining to professional work." The IEEE Code of Ethics (1990) includes such principles as "avoid real or perceived conflicts of interest whenever possible" and "be honest and realistic in stating claims or estimates based on available data."

The Accreditation Board for Engineering Technologies (ABET) has long required an ethics component in the computer engineering curriculum. And in 1991, the Computer Sciences Accreditation Commission/Computer Sciences Accreditation Board (CSAC/CSAB) also adopted the requirement that a significant component of computer ethics be included in any computer sciences degree granting program that is nationally accredited [Conry, 1992].It is clear that professional organizations in computer science recognize and insist upon standards of professional responsibility for their members.

VI. CONCLUSION

When creating an ethics strategy, it is important to look at the regulatory requirements for ethics programs. These provide the basis for a minimal ethical standard upon which an organization can expand to fit its own unique organizational environment and requirements. The purpose of an effective compliance and ethics program is "to exercise due diligence to prevent and detect criminal conduct and otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law." The new requirement significantly expands the scope of an effective ethics program and requires the organization to report an offense to the appropriate governmental authorities without unreasonable delay.

VII. REFERENCES

[1] http://www.techterms.com/definition/computerethics
[2] http://dehn.slu.edu/courses/fall06/493/ComputerEthics.html.
[3] Gotterbarn, Donald (1991) "Computer Ethics: Responsibility Regained," National Forum: The Phi Beta Kappa Journal, Vol. 71, 26-31.
[4] Gotterbarn, Donald (2001) "Informatics and Professional Responsibility", Science and Engineering Ethics, Vol. 7, No. 2.
[5] Nissenbaum, Helen (1998) "Protecting Privacy in an Information Age: The Problem of Privacy in Public," Law and Philosophy, Vol. 17, 559-596.
[6] Nissenbaum, Helen (1999) "The Meaning of Anonymity in an Information Age," The Information Society, Vol. 15