

Computer Ethics: an Argument for Rethinking Business Ethics

Wanbil W. Lee¹ and Allan K.K. Chan²

¹Honorary Associate, School of Business, Hong Kong Baptist University
Hon. Research Associate, Information Security & Cryptography, Hong Kong University

²Associate Dean and Professor, School of Business, Hong Kong Baptist University

Abstract

Computers change our life at personal, social and international level. The outcome of these changes may be beneficial or harmful, and are often beyond our anticipation. This raises questions of right or wrong, good or bad. These questions often defy explanations based on traditional moral doctrines and long adopted business conventions. We studied the impact of computers on traditional ethical principles. We also studied the ethical implications arising from managing information security. We found grounds that arguably support our assertion.

INTRODUCTION

This paper argues for rethinking the values of business ethics because issues surrounding computer applications flout extant moral norms. The conclusion of the argument infers from a three-fold premise. The first premise argues for the need of a computer ethics due to impact of the computer. The second premise asserts that there exists impact of computer ethics on information security management. The third premise argues for the linkage of computer ethics to corporate policy, on grounds that that information is recognized as an important corporate asset such that information protection is vital, information security is an integral part of a corporate policy, and information security management is an essential element of the overall corporate management. This three-fold premise thus leads to the conclusion of rethinking business ethical values. (See Figure 1 below)

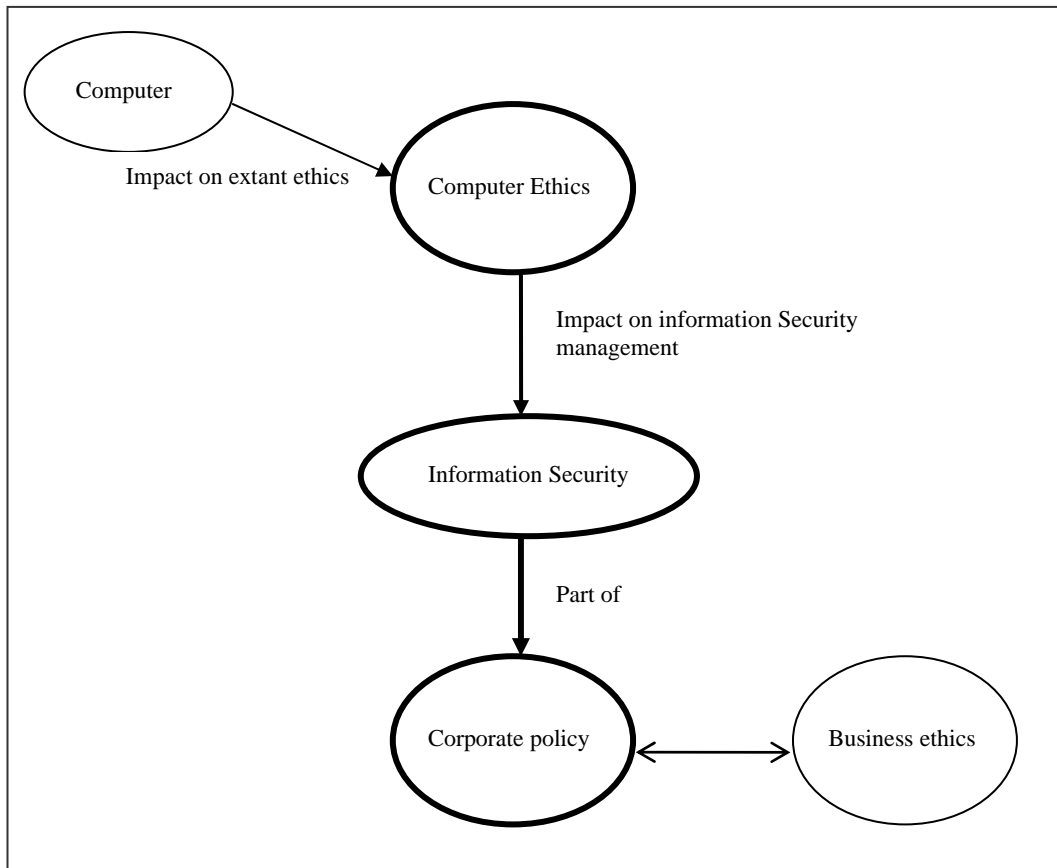


Figure 1 – Linking Computer Ethics, Information Security and Corporate Policy

ARGUMENT

Premise 1 – the need for a computer ethics

Of all technologies invented since civilization, the computer is the only one that extends our intellectual power and all the others extend our physical power. For example, the steam engine extends our arms to “lift heavy loads”, the automobile strengthens our legs to “walk faster”, and the telephone raises our voice and extends our hearing power to talk and listen to some one over a distance, respectively, but the computer makes us smarter to draw inference or deduce conclusions from cross-referencing a vast amount of data stored in a data mine, and bolsters our memory by being to recall readily and consistently from the data mine. Thus the computer is considered to be able to think, and is called a thinking machine in some

quarters in our society.

The computer changes the way we communicate, the way we are educated, the way we are entertained, and the way we work and run our business. The changes due to the applications of the computer, like other technologies, often produce effects that we didn't anticipate and which may be beneficial but may also be harmful. This raises the issue of the right way or the wrong way of applying the computer, or applying the computer to bring about effect that is good or bad to society. This issue has spurred ethicists to think about a computer ethics.

So, what is Computer Ethics? Given that *ethics* refers to concerns about *what people should do*, about value or goodness of things and situations, and about justice (formal and informal), Computer Ethics is “the analysis of the nature and social impact of computer technology and the corresponding formulation and justification of policies for the ethical use of such technology” (Moor, 1995, p. 7). A more modern definition is proposed by Johnson (2001), which is the study of *what people should do surrounding computers* about the ethical issues raised therein, grounded in ordinary moral principles, and perhaps an extension of these principles to situations created by computers.

Now that we are clear about what Computer Ethics is and why we need it, we face a policy *vacuum* about how computers should be used rightly because traditional ethics become inadequate as computer applications proliferate (Moor, 1995). To fill this vacuum necessitates modifications of existing ethical rules and perhaps addition of new ones.

There are three noteworthy reasons. The first is that utilizing this “thinking power” – the development and deployment of the computer – raises questions of ethics (as already pointed out earlier in this paper). This necessitates identifying and bringing into focus the issues and problems, thus raising awareness of the ethical dimension, of a particular situation. Then, there is need to provide an approach to advancing our understanding of these issues and problems, and to suggest ways of

reaching wise solutions. For example, it is now possible for anyone to violate my privacy, to sabotage my files, or to steal my idea, without entering my home or office. Consequently, I am responsible to protect my confidential information, by means of my password in addition locking my home and office. This inadequacy or lack of guidelines to address these ethical questions is described as a vacuum of ethical rules or policies created by the computer (Moor, p. 8). To fill the vacuum with rules and laws based on ethical principles is why we have computer ethics.

Second, some people argue that computers are unique in that they are different from other technologies (as pointed out earlier) and their unique characteristics render traditional ethical concepts and theories inappropriate. Furthermore, computers are unique because they are “inherently unreliable” and malleable (Moor, p. 10). Others argue that computers are not new or not unique because any problems of ethics involving computers are like old wine in a new bottle or with a somewhat different twist. Hence, the work of computer ethics is not to create a new system of ethics but rather to apply traditional ethics and to extend them to cover situations that are attributed to computers. This makes another reason that study of computer ethics is necessary.

Third, although computer professionals often do not have much power individually, yet they have collective power by virtue of their special position in an organization in particular, and in society in general, because of their expertise. This is a powerful influence on the directions of development, use, and attitude towards computers. However, responsibility for social and ethical implications of computing should not be delegated to computer professionals only, and the public should be educated, so that both computer professionals and laymen understand computers and appreciate the associated social and ethical implications and will equally be responsible when participating in a democratic process. This further reinforce the importance of why computer ethics.

Premise 2 – ethical impact on information security

As the technology advances, such as the Internet, which has changed the rules for security¹, and as the hackers and crackers are always lurking to find a loophole

somewhere, the extant Control Tools become impotent and new tools are continuously needed. In addition, as legislations always lag behind the event, new laws are required. Though slow and time consuming, yet progress of developing new tools and new laws has been incremental. In the case of Computer Ethics, its adoption is even slower. However, despite the potential barriers to and the difficulties in the application of ethical principles in information security management, it is argued that i) there exists a *relationship* between Computer Ethics and Information Security and ii) it is necessary but not sufficient to trust people just by setting a number of ethical rules, and *education* may help towards ethical awareness and action², such that Computer Ethics may actually and not just theoretically help information security management.

The relationship between Information Security and Computer Ethics does not look, on the surface, readily obvious, or even appears remote. It is, however, credible as shown in Figure 2 below.

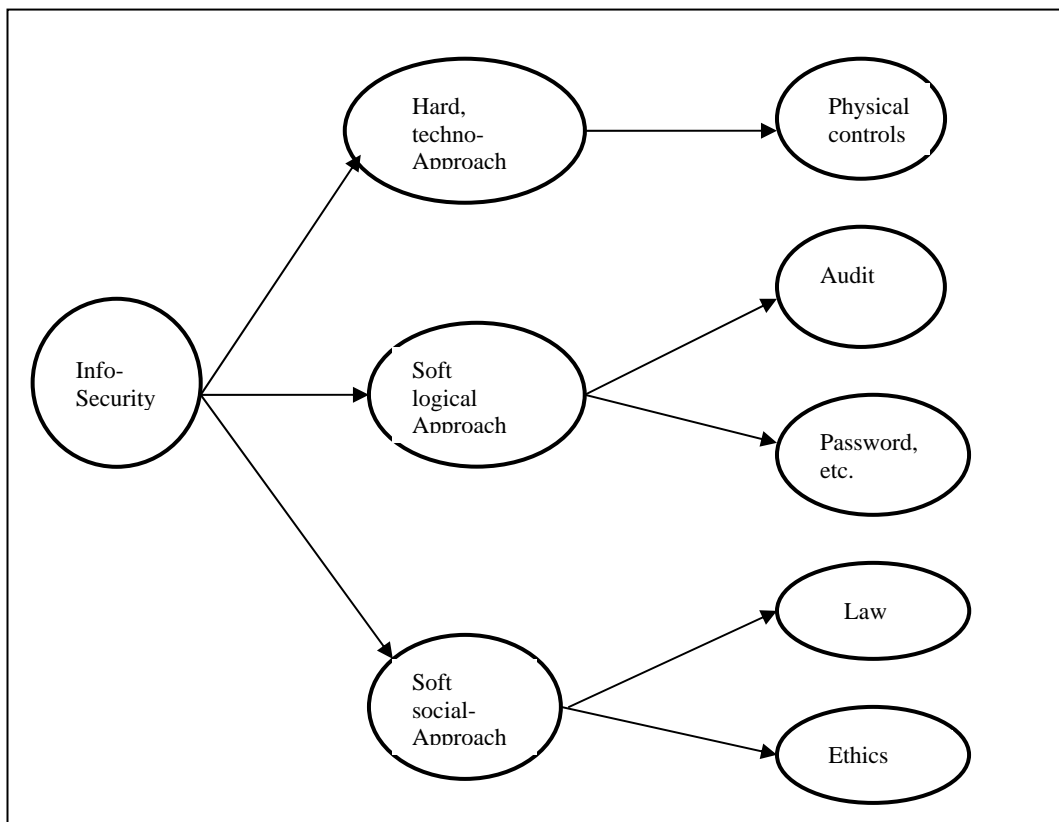


Figure 2 – Position of Ethics relating to Information Security

It is credible in view of the following: i) culture, customs, trust, and privacy that characterize security fall within the realm of ethics and ii) Computer Ethics alerts Information Security Management to ethical consideration and warns off potential offenders of ethical consequences in situations where the technical tools or the legal measures fail but an ethical decision may be helpful in bringing about a solution. This premise is consistent with the following three observations:

First, the Information Security Management community has applied *control tools* to meet the information security objectives of safeguarding confidentiality against unauthorized access, upholding integrity and maintaining availability. However, detecting computer crime is difficult because the act is either traceless or hard to trace. Quantifying the damage is problematic because the victims all too often withhold reporting the crime for fear of recrimination, bad publicity and so on (Lee, 1997). Therefore, the technical control tools are ineffective with respect to legal issues.

Second, computer laws have been enacted in various nations at an ever increasing rate since the late 1980s when the business in particular and society at large were forced to face the magnitude and severity of the damage not experienced before the attacks of computer crimes (Bainbridge, 2004). There has been a dramatic increase in specialized legislations to combat the criminal behaviors due to computer crime, which includes traditional crimes committed with the use of a computer as well as a variety of new, technology-specific criminal behaviors spawned by the rapid emergence of computer technologies, and an exponential expansion of the Internet (Ditzion et al., 2003). However, despite the additional new laws, prosecution is deterred because the legal proceeding is a tardy, time-consuming and expensive process even when there are well-justified intentions to proceed with legal action. Also, legislation always lags behind the event such that either we find no appropriate laws, or the new law is too late, for the case in hand. Hence, Computer Laws is at best a deterrent to computer crime, not a guardian of information.

Third, computer ethicists assert on the one hand that special ethical issues are raised because computers are special technology, and query on the other hand why there should be Computer Ethics since, for example, there is no such thing as

Telephone Ethics even though the telephone is a special technology that makes a profound change on the way we communicate with others (Maner, 2001). However, information security is worthy of ethical consideration as many decisions in information technology affect a wide range of stakeholders. National and international computer societies had promoted codes of ethical practice, and even written these codes into their constitutions (Cardinali, 1995). Notably, the Association for Computing Machinery and the Institute of Electrical and Electronic Engineers-Computer Society developed in 1998 the *ACM/IEEE Software Engineering Code of Ethics and Professional Practice* in terms of eight principles³. Guidelines for ethical practice are laid down by various international and national bodies, and these guidelines are similar in spirit, cover similar grounds, but may comprise different number of items and are composed of different wordings, for example, ACM's *Code of Ethics*, the current version of which was adopted in 1992⁴; *Code of Ethics and Professional Conduct* by the Japan Information Technology Service Industry Association⁵; *Code of Ethics and Professional Conduct* by the Hong Kong Computer Society⁶. The British Computer Society issues two documents: *Code of Good Practice and Code of Conduct*⁷; the Australian Computer Society produces a series of ethical case study⁸. While such codes may serve to deter potential offensive actions, they are limited because they rely purely on the moral obligation of the members because even though violation of professional conduct may result in expulsion from the societies or termination of membership benefits and privileges, violation by itself does not attract any criminal charges in the legal sense. That these codes exist do help to reduce the incidence of abuse, fraud and software piracy. Even though adoption of the codes cannot guarantee more ethical behavior, the codes of ethical professional conduct are nonetheless contributive to information security.

Premise 3 – information security a part of corporate policy

In the contemporary context, business corporations increasingly rely on their computer-based information systems to conduct themselves and to make decisions. Executive management has urged business corporations to ensure a secure system,

lest the data are vulnerable to unauthorized access and inappropriate disclosure (confidentiality aspect of information), disruption or illegal utilization (availability aspect of information), and improper modification (integrity aspect of information), and decisions based on insecure and unreliable information can lead to disastrous consequences. Enforcing confidentiality, upholding integrity and ensuring availability rely on assumptions and trust. It is assumed that the data are correct and trustworthy, and any attempt to deny service is atypical; at the same time, trust exists only when a security policy has been formally endorsed and a security mechanism is functionally sound (Bishop, 2005). In other words, given that information is a key corporate asset, information protection is a critical corporate operation, and information security a core corporate policy. It follows that any disturbance to the confidentiality, integrity and availability of information will necessitate adjustment the intensity of information protection measures, any impact (due to computers and others) on the operation (i.e., information protection) will alarm the policy (i.e., information security), and any change in policy will result in the way we run the business – the way right or the wrong way. This arouses thinking or rethinking of our value judgment, value of business ethics.

CONCLUSION

We have argued for a computer ethics (Premise 1). We have also argued for the contribution made by ethical thinking on information protection (Premise 2), which echoed the conclusion reached by Lee and Chan (2008). Finally, we argue that there is change to the values of traditional ethics, given that there exists the impact due to computers on information security, one the core corporate policies in the contemporary context (Premise 3). The premises have led to positive conclusions, thus the urge to think again the values of business ethics. The summary is depicted in Figure 3 below.

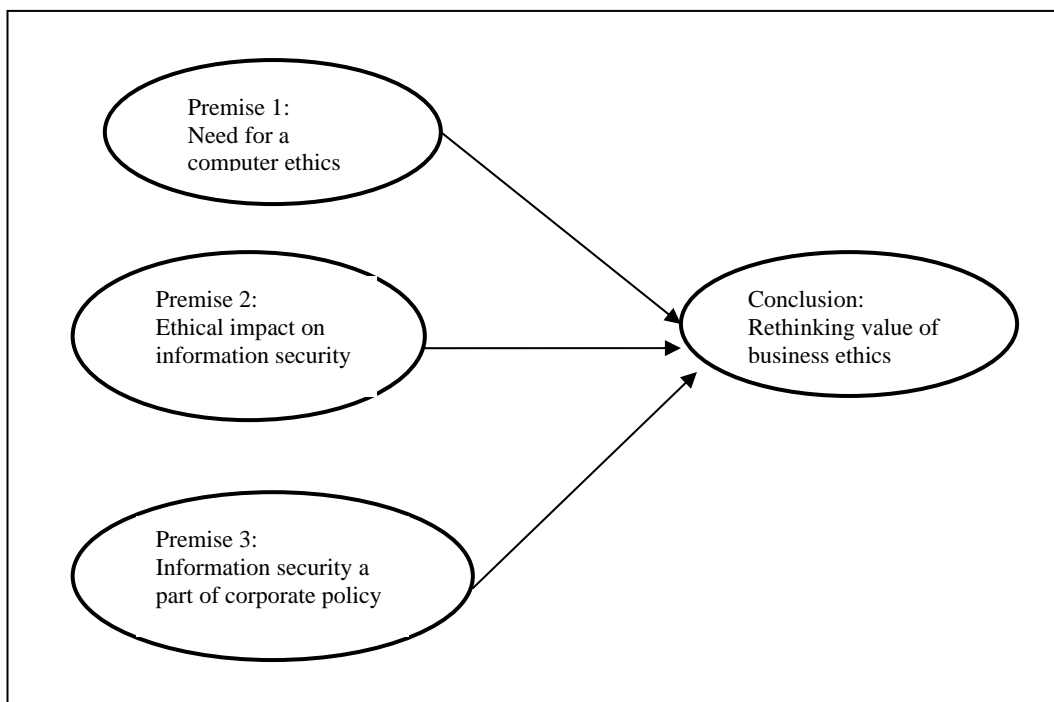


Figure 3 – Summarizing the Conclusion

This paper should be of interest to those who have the responsibility to formulate corporate policy for information protection, and to business executives who are aroused to review the values of business ethics in light of applying modern technologies, in particular, computers.

FOOTNOTES

¹Bitpipe Inc., “Preemptive Protection: Changing the Rules of Internet Security: White Paper” published by Internet Security Systems[®], 19 October 2004 (http://www.bitpipe.com/detail/RES/1083349267_979.html?src=mu.ij, 20 November 2004).

²Lee and Chan (2008) present some preliminary empirical data based on a mini survey that aims to assess the effect of ethics in the work place and role of education. The participants were part-time final year students for an undergraduate award in Computing at the Hong Kong Polytechnic University, aged ranging from early 20s to early 40s, in regular full-time positions in the

computer industry ranging from help-desk consultant to manager of an installation. The survey was carried out at the beginning and at the end of a compulsory course that includes topics of ethics and professionalism. The same questionnaire was used in two consecutive academic years: 2006/07 (71 students) and 2007/08 (90 students). The responses are fairly consistent between the two cohorts. Before attending the course, the majority of participants admitted that they never heard or aware of computer ethics or nor sure if they carried out work ethically. After the course, the majority of participants claimed that they understood (i.e., learned) computer ethics and would conduct work according to ethical principles. There is *prima-facie* evidence of a positive effect by education.

³Refer <http://www.acm.org/about/se-code> for a detailed decryption of the elements that make up the eight principles

⁴Refer <http://www.acm.org/about/code-of-ethics> for further details of the rules and regulations (current version). See also Anderson, R., “The ACM Code of Ethics: History, process, and implications”. In *Social Issues in Computing*, Huff, C. and Finholt, T. (Eds), McGraw Hill, New York, 1994, pp 48-71. In his paper, Anderson provided an account of the history and analysis of the current version (adopted in 1992) and compared the current version and the original version (developed in 1972).

⁵<http://www.jisa.or.jp/en/introduction/ethics.html> (15 March 2008)

⁶<http://www.hkcs.org.hk/ethics.htm> (15 March 2008)

⁷<http://www.bcs.org/server/php?show=nav.6029> (15 March 2008)

⁸<http://www.wacs.org.au/index.cfm?action=list&groID=casestudy> (15 March 2008)

REFERENCES

- Bainbridge, D.: 2004, *Introduction to Computer Law*, 5th edition (Pitman, London).
- Bishop, M. A.: 2005, *Introduction to Computer Security* (Addison Wesley, Boston).
- Cardinali, R.: 1995, “Reinforcing our Moral Vision: Examining the Relationship between Unethical Behaviour and Computer Crime”, *Work Study*, 44 (8), pp 11-17.

- Ditzion, R., E. Geddes, and M. Rhodes: 2003, "Computer Crimes", *The American Criminal Law Review*, 40(2), pp. 285-337.
- Johnson, D.G.: 2001, *Computer Ethics* 3rd edition (Upper Saddle River, NJ: Prentice-Hall).
- Lee, Wanbil W.: 1997, "A Deterrent Measure Against Computer Crime: Knowledge-Based Risk-Analytic Audit", *Singapore Management Review*, January, pp 19-45.
- Lee, Wanbil W. and Keith C.C. Chan: 2008, "Computer Ethics: a Potent Weapon for Information Security Management", *The Information Systems Control Journal*, Volume 6 (December).
- Maner, W.: 2001, "Unique Ethical Problems in Information Technology", in D.M. Hester and P.J. Ford (eds.), *Computers and Ethics in the Cyberage* (Upper Saddle River, NJ: Prentice-Hall), pp 39-56.
- Moor, J.M.: 1995, "What is Computer Ethics?" in D.G. Johnson and H. Nissenbaum (eds.), *Computer Ethics & Social Values* (Upper Saddle River, NJ)