INFORMATION SECURITY AND ETHICS IN EDUCATIONAL CONTEXT: THE DEVELOPMENT OF CONCEPTUAL FRAMEWORK TO EXAMINE THEIR IMPACT

Meysam Namayandeh[a], Maslin Masrom[b], and Zuraini Ismail[b]

[a]Centre for Advanced Software Engineering, University Technology Malaysia

[b]Department of Science, College of Science and Technology, University Technology Malaysia

ABSTRACT

Information security and ethics are viewed as major areas of interest by many academic researchers and industrial experts. Information security and ethics is defined as an all-encompassing term that refers to all activities needed to secure information and systems that supports it in order to facilitate its ethical use. In this research, the important part of current studies introduced and the fundamental concepts of a security framework are explained. To achieve the goals of information security and ethics, suggested framework discussed from educational level to training stage in order to evaluate computer ethics and its social impacts. Using survey research, insight is provided regarding the extent to which and how university student have dealt with issues of computer ethics and to address the result of designed computer ethics framework on their future career and behavioural experience.

1. INTRODUCTION

The current development in information and communication technologies have impacted all sectors in our daily life where does not matter whether it is technical or routine. To ensure effective working of information security, various controls and measures had been implemented as the current policies and guidelines between computer developers (Hamid, 2007). However, lack of proper computer ethics within information security is affecting educational society day by day.

Undoubtedly, the most important of these controls is to define an understandable framework or model for students who roles future computer engineer or scientist. Hence, this project examines awareness and information of students in computer ethics from educational aspect. Also from Malaysian perspective, review of related research (Maslin & Zuraini, 2008) indicates the existence of conflicting views concerning the ethical perceptions of students. In today's global economy, computer security and computer ethics awareness is an important component of any management information system (North, et al. 2006).

It would an undeniable element of security in Malaysian computer technology as Malaysia is ranked 8 out of 10 top infected countries in the Asia Pacific region as a target for cyber attackers (Sani, 2006). Indeed, points out that there is a need to understand the basic cultural, social, legal and ethical issues inherent in the discipline of computing. For these reasons, it is essential that as a future computer professionals are taught the meaning of responsible conduct (Langford, 2000).

As the computer ethics was one of the major topics which have been throughout the past decades, in order to prevent the people from the social impact, therefore in this part of introduction, we have a short milestone on computer ethics and related history of designed. During the late *1970s*, Joseph Weizenbaum, a computer scientist at Massachusetts Institute of Technology in Boston, created a computer program that he called ELIZA. In his first experiment with ELIZA, he scripted it to provide a crude imitation of a psychotherapist engaged in an initial interview with a patient. In the mid 1970s, Walter Maner began to use the term "computer ethics" to refer to that field of inquiry dealing with ethical problems aggravated, transformed or created by computer technology.

Maner offered an experimental course on the subject at University. During the late 1970s, Maner generated much interest in university-level computer ethics courses. He offered a variety of workshops and lectures at computer science conferences and philosophy conferences across America.

By the *1980s*, a number of social and ethical consequences of information technology were becoming public issues in the world, issues like computer-enabled crime, disasters caused by computer failures, invasions of privacy via computer databases, and major law suits

regarding software ownership. Because of the work of Parker and others, the foundation had been laid for computer ethics as an academic discipline. In the mid-80s, James Moor of Dartmouth College published his influential article "What is Computer Ethics? In Computers and Ethics, a special issue of the journal on that particular time.

During the *1990s*, new university courses, research centers, conferences, journals, articles and textbooks appeared, and a wide diversity of additional scholars and topics became involved. The mid-1990s has heralded the beginning of a second generation of Computer Ethics which contain the new concept of security. The time has come to build upon and elaborate the conceptual foundation whilst, in parallel, developing the frameworks within which practical action can occur, thus reducing the probability of unforeseen effects of information technology application.

In *2000s*, the computer revolution can be usefully divided into three stages, two of which have already occurred, the introduction stage and the permeation stage. The world entered the third and most important stage "the power stage" in which many of the most serious social, political, legal, and ethical questions involving information technology will present themselves on a large scale. The important mission in this era is to believe that future developments in information technology will make computer ethics more vibrant and more important than ever. Computer ethics is made to research about security and it's beneficial aspects.

The remainder of this paper is organized as follows: section 2 describes the details of DAMA frame work by further phases on section 3. In section 4 the related theories are discussed from ethical views.

2. FRAMEWORK

We have developed a framework for development of information security with computer ethics respect to educational conception. The further discussion follows the exact code of ethics which are including Privacy, Property, Accuracy and Accessibility. As Fig. 1 depicts, DAMA (Delimma, Attitude, Morality, Awareness) framework examines information security and computer ethics from two major dimensions: *the educational* and *security training*. In addition DAMA framework are also explored to suggested the educational core of computer ethics which is the effective ways to teach information security along with computer ethics from the basis of educational level rather than higher level.

The educational dimension is focusing on the core of information security which considers along with *awareness*, *morality*, *attitude* and *dilemma*. In fact, educational dimension is explored from various perspectives to have relevance for group rather than individuals where the main focus of this issue has been mentioned in training level. Examples of questions in order to guide the development of DAMA framework references include: have you ever heard about computer ethics? What are ethical dilemmas and its social impacts?

The other main phase of educational dimension is moral development that includes personal beliefs related to their background of computer ethics. In fact, it focus on morality and further effectiveness that how individual morality can change their attitude and therefore acquire appropriate awareness hence evaluate ethical dilemmas.

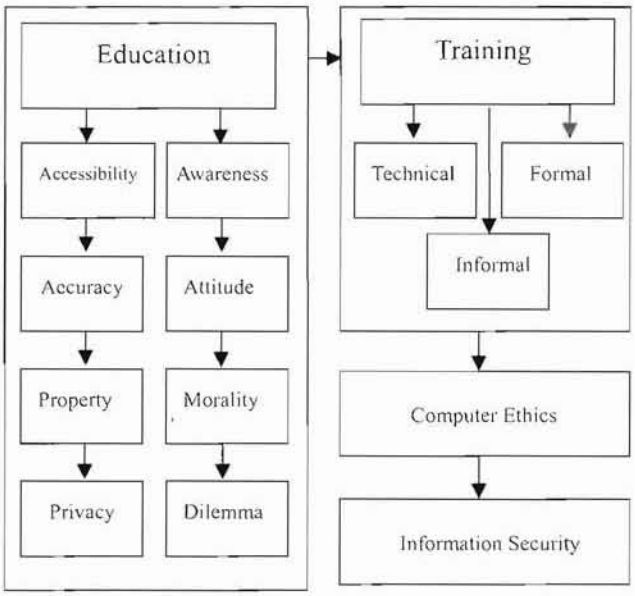

Fig. 1 DAMA Framework.

Moreover, security and training dimension is what students themselves manifest core of information security along with the help of formal and informal discussion. The security dimension includes informal discussion of common mistakes that happens among most of security consultant and officers which are relevant to information security ethics. It includes discussions of specific exploits of current weaknesses and may result as unethical behaviour. The goal of security dimension is to communicate students from technical perspective to theoretical training.

DAMA approaches present methods and creative ideas for teaching of computer ethics with respect of information security for diverse audiences. The framework's dimensions cover the basic levels for computer ethics lectures and class room discussions related to ethical behaviour of future computer scientists. The main emphasis is to presents creative and beneficial methods for learning experiences in various kinds of information security ethics. The authors place particular focus that will require students to build and rebuilt their beliefs in different ways in order to know unethical behaviours and their social impact on their future career.

3. EDUCATIONAL DIMENSION

3.1 DAMA

Computer education now begins in elementary school and is no longer a restricted technical specialty learned

only by those who are going to design or program computers. Because of the widespread prevalence of computers in society a core of ethical precepts relating to computer technology should be communicated not only to computer professionals, but to the general public through all levels of education. The issue should be viewed from the perspective of society and perspective of computer professionals (Spinello, 2003).

In looking at the computer ethics there is a great emphasis upon incorporating ethical and social impact issues throughout the curriculum starting at the point when children first become computer users in school. In particular, there are a set of guidelines regarding what students in general need to know about computer ethics. The preparation of future computer professionals should be examined at both the high school and university computer science curriculum (Forcht, et al., 2004).

The researchers (Maslin & Zuraini, 2008) are in the process of developing new recommendations at both levels of curriculum. In the high school curriculum, there will be both general and specific approaches to ethics and social impact issues.

The general approach is to incorporate these concerns across the curriculum, not just in computer courses. This is in keeping with the philosophy that computers should be integrated across the curriculum as a tool for all disciplines. The specific approach is to develop social impact modules within the computer courses that will focus on these concerns (Foster, 2004).

At the university level the researchers faces a yet-to-be resolved dilemma of how to implement the proposed societal strand in the new curriculum recommendations. There is much discussion, but little action, regarding the necessity of preparing ethically and socially responsible computer scientists, especially in light of the highly publicized computer viruses that are an embarrassment to the profession. When combined with other computer science core material, the teaching of ethics is made complicated by the fact that it is not as concrete as the rest of the curriculum. In accepting the value-laden nature of technology, researchers should recognize the need to teach a methodology of explicit ethical analysis in all decision-making related technology. The moral development is at the heart of interest in the morality element. In this model (Dark, et al., 2006), researchers wanted to create educational opportunities that allow students to examine their existing beliefs regarding ethical and technical issues and in relation to existing technical, professional, legal, and cultural solutions. In an earlier section, it described how students examine these solutions with an external, objective point of view.

Now, the student is positioned at the centre of the intersecting circles. The is aim to create educational opportunities that allow and encourage students to explore "who am I now" in relation to technical, professional, cultural, and legal solutions to these ethical and security issues, and asks questions such as "what is the relationship between who am I, who I want to be, and these issues and solutions"?

The most important factor in effective computer security is people's attitudes, actions, and their sense of right and wrong (Huff & Frey, 2005). Problems and issues raised in the computing environment, Topics to be discussed include misuse of computers, concepts of privacy, codes of conduct for computer professionals, disputed rights to products, defining ethical, moral, and legal parameters, and what security practitioners should do about ethics.

The issue of computer security has fallen into the gray area that educators and industry alike have avoided for fear that too little knowledge could be hazardous and too much could be dangerous. Most organizations acknowledge the need for data security, but, at the same time, approach security as hardware. It may be more important, and far more successful to address the issue of data security as an attitude rather than a technology.

3.2 PAPA

According to (Mason, 1986) decision makers place such a high value on information that they will often invade someone's privacy to get it. Marketing researchers have been known to go through people's garbage to learn what products they buy, and government officials have stationed monitors in restrooms to gather traffic statistics to be used in justifying expansion of the facilities.

These are examples of snooping that do not use the computer. The general public is aware that the computer can be used for this purpose, but it is probably not aware of the ease with which personal data can be accessed. If you know how to go about the search process, you call obtain practically any types of personal and financial information about private citizens. Here four major aspect of Mason's theory shall be studied:

3.2.1 Privacy

Privacy may define as the claim of individuals to determine for themselves when, to whom, and to what extent individually identified data about them is communicated or used. Most invasions of privacy are not this dramatic or this visible. Rather, they creep up on us slowly as, for example, when a group of diverse files relating to a student and his or her activities are integrated into a single large database.

Collections of information reveal intimate details about a student and can thereby deprive the person of the opportunity to form certain professional and personal relationships. This is the ultimate cost of an invasion of privacy. So why integrate databases in the first place. It is because the bringing together of disparate data makes the development of new information relationships possible.

3.2.2 Accuracy

Accuracy represents the legitimacy, precision and authenticity with which information is rendered. Because of the pervasiveness of information about individuals and organizations contained in information systems, special care must be taken to guard against errors and to correct

known mistakes. Difficult questions remain when inaccurate information is shared between computer systems. Any framework should describe the legal liability issues associated with information. Who is held accountable for the errors? This is an important question may come across every researcher's mind or which party liable for inexact or incorrect information that leads to devastation of another.

3.2.3 Property

One of the more controversial areas of computer ethics concerns the intellectual property rights connected with software ownership. Some people, like Richard Stallman who started the Free Software Foundation, believe that software ownership should not be allowed at all. He claims that all information should be free, and all programs should be available for copying, studying and modifying by anyone who wishes to do so. Others argue that software companies or programmers would not invest weeks and months of work and significant funds in the development of software if they could not get the investment back in the form of license fees or sales (Mason, 1986).

Today's software industry is a multibillion dollar part of the economy; and software companies claim to lose billions of dollars per year through illegal copying. Many people think that software should be own able, but "casual copying" of personally owned programs for one's friends should also be permitted. The software industry claims that millions of dollars in sales are lost because of such copying.

3.2.4 Accessibility

Accessibility represents the legitimacy, precision and authenticity with which information is rendered. Regarding this important aspect of research this question may come across the people's mind who is held accountable for errors? Who can you trust in order to outsource your project? In fact, in term computer ethics accessibility means, what kind of information would available for the legal users and students.

4. SECURITY AND TRAINING LEVEL

In terms of computer ethics, security would be an undeniable factor of it. Therefore, short review on information security which is influence in computer ethics will help the researcher to identify the further study. Many different terms have been used to describe security in the IT areas where information security has become a commonly used concept, and is a broader term than data security and IT security. Information is dependent on data as a carrier and on IT as a tool to manage the information.

Information security is focused on information that data represent, and on related protection requirements. So the definition of information system security is "the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats". Four characteristics of information security are: availability, confidentiality, integrity and accountability, simplified as "the right information to the right people in the right time". *Availability:* concerns the expected use of resources within the desired timeframe. *Confidentiality:* relates to data not being accessible or revealed to unauthorized people *Integrity:* concerns protection against undesired changes. *Accountability:* refers to the ability of distinctly deriving performed operations from an individual. Both technical and administrative security measures are required to achieve these four characteristics.

4.1 Technical level security

From a technical perspective, the preservation of confidentiality, integrity availability and accountability requires the adoption of IT security solutions such as encryption of data and communication, physical eavesdropping, access control systems, secure code programming, authorization and authentication mechanisms, database security mechanisms, intrusion detection systems, firewalls. At this level it is possible to introduce frameworks and methods for the selection of the appropriate technological solution depending on the needs for a particular application with respect to security in computer ethics.

4.2 Formal level security

The formal level of information security is related with the set of policies, rules, controls, standards, etc. aimed to define an interface between the technological subsystem (Technical level) and the behavioural (computer ethics) subsystem (Informal level).

According to many definitions of an information security, this is the level where much of the effort of the information security is concentrated. An interesting review of the security literature identifies a trend in information system research moving away from a narrow technical viewpoint towards a socio-organizational perspective.

4.3 Informal level security

In the domain of the informal level of information security, the unit of analysis is individual and the research is concerned about behavioural issues like values, attitude, beliefs, and norms that are dominant, and influencing an individual employee regarding security practices in an organization. The solutions suggested in this domain are more descriptive than prescriptive in nature and the findings at this level need to be effectively implemented through other levels (i.e. formal and technical). An interesting review of research papers in the behavioural or computer ethical domain is, looking at used theories, suggested solutions, current challenges, and future research (Bynum, 2006) .

5. THEORIES PERSPECTIVE

Ethics is an important facet of comprehensive security of information system's security. Research in ethics and information systems has been also carried outside the information security community. Anyhow, researcher sees that the relationship of hackers and information security personnel has not yet been properly analyzed. Within this short review, a philosophical point of view shall be taken, and problems of establishing ethical protection measures against violations of information security shall be studied.

Further analysis leads to quite opposite results of the main stream arguments that support the need of common ethical theories for information security. This addition provides with a framework that is feasible within the current technology, supports natural social behaviour of human beings and is iterative enabling forming of larger communities from smaller units.

Recently, the trend appears to be that the ethics approved by the security community is having the law enforcement (Cruz & Frey, 2004). Several attempts around the world are made to enforce proper behaviour in the information society by theoretical methods. From 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 (Fowler, 2004). Further depth into the conflict can be found by introducing another dimension to the classification of ethical theories into two categories: Phenomenologist vs. Positivist and individualist vs. collectivist ethics.

Phenomenologism vs. Positivism: According to the phenomenological school, what is good is given in the situation, derived from the logic and language of the situation or from dialogue and debate about "goodness". Positivism encourages s to observe the real world and derive ethical principles inductively.

Individualism vs. Collectivism: According to the individualistic school, the moral authority is located in the individual whereas collectivism says that a larger collectivity must care the moral authority. Major schools, based on these concepts, can be listed to be Collective Rule-Based Ethics, Individual Rule- Based Ethics. A detailed analysis of these schools is provided by (Leiwo & Heikkuri, 1998).

Also from distributed information systems perspective security of information systems requires both technical and non-technical measures, special effort must be paid on the assurance that all methods support each other and do not set contradictory or infeasible requirements for each other which contain two major theoretical elements:

Ethics negotiation phase is where organizations or individuals representing themselves negotiate the content of ethical communication agreement over specific communication channels.

Ethics enforcement phase is where each organization enforces changes in the ethical code of conduct by specifying administrative and managerial routines, operational guide lines, monitoring procedures, and sanctions for unacceptable behaviour. Organizations or university individuals involved in negotiation should code desired ethical norms in terms of acceptable behaviour within the information processing. Agreement should be searched and once reached, contract made and agreed norms enforced throughout the organization. In the optimal case, ethics has the law enforcement and juridical actions against violations can be prosecuted in court.

6. CONCLUSION

Educational centers within higher educational level have unique opportunity to help and educate computer users in order to face with ethical dilemmas. Therefore, this would be the main challenge of this study to focus on computer ethics with the help of suggested framework. As a result, computer ethics is becoming a field in need of research based upon a necessity to provide information for education which is related to security concepts. The legal structure appears to be limited in its ability to provide ethical behaviour effectively. While not wishing to be alarmists, research suggests the needs to be concerted effort on the part of the all the computer professional societies to update their ethical codes and to incorporate a process of continual security.

REFERENCES

Bynum, T., Computer ethics: Basic concepts and historical overview, Stanford, *Encyclopedia of Philosophy*. 2006.

Cruz, J., and Frey, W., An effective strategy for integrating ethics across the curriculum in engineering, *An ABET 2000 Challenge, Science and Engineering Ethics*, vol. 9, no. 3, pp. 543-568, 2004.

Dark, M., Epstein, R., Morales, L., Countermine, T., Yuan, Q., Ali, M., Rose, M., and Harter, N., A framework for information security ethics education, *Proc. Of the 10th Colloqium for Information Systems Security Education*, University of Maryland, University College Adelphi, MD June 5-8, 2006.

Forcht, K. A., Pierson, J. K., and Bauman, B. M., Developing awareness of computer ethics, *ACM*, 1998.

Foster, A. L., Insecure and unaware, *The Chronicle of Higher Education*, (May 7, 2004), p. 33.

Fowler, T. B., Technology's changing role in intellectual property rights, *IT Pro4*, vol.2, pp. 39-44, 2004.

Hamid, N., Information security and computer ethics: Tools, theories and modeling, North Carolina University , *Igbi Science Publication*, vol. 1, pp. 543-568, 2007.

Huff, C., and Frey, W., Good computing: A

pedagogically focused model of virtue in the practice of computing, *Under Review*, pp. 30-32, 2005.

Langford, D., Practical computer ethics, *London*: McGraw Hill, pp. 118-127, 2000.

Leiwo, J., and Heikkuri, S., An analysis of ethics as foundation of information security in distributed systems, *Proc. 31st Annual Hawaii International Conf. on System Sciences*, pp. 213-222, 1998.

Maslin M., and Zuraini, I., Computer security and computer ethics awareness: A component of management information system, *Malaysia Conf. IEEE Technology and Society Magazine*, 2008.

Mason, R. O., Four ethical issues of the information age, *Management Information Systems Quarterly*, vol. 10, no. 1, pp. 5-12, 1986.

North, M. M., George, R., and North, S. M. Computer security and ethics awareness in university environments: A challenge for management of information systems, *ACM*, Florida, United States of America, pp. 434-439, 2006.

Sani, R., Cybercrime Gains Momentum, *New Straits Times*, April 3, 2006

Spinello, R., Cyberethics: morality and law in cyberspace, Third edition, Sudbury, vol. 2, 2003.

Meysam Namayandeh received the BSc Computer Science (2006) from N. Wadia College, University of Pune, India. He is a graduate student (Master of IT Security), Centre for Advanced Software Engineering, University Technology Malaysia ***International Campus***, Kuala Lumpur. His current interests include information security and computer ethics.

Maslin Masrom received the BSc Computer Science (1989), MSc Operations Research (1992), and PhD in Operations Mgmt/Mgmt Info System (2003). She is a Senior Lecturer, Department of Science (Computer Science Unit), College of Science & Technology, University Technology Malaysia *International Campus*, Kuala Lumpur. Her current interests include information system/information technology management, ethics in computing, e-learning, and structural equation modeling.

Zuraini Ismail received her B. Sc. in Management Info System (1984), M. Sc. in Computer Info Systems (1987), and Ph.D. in Management Info Systems (2007). She is a Senior Lecturer at Department of Science (Computer Science Unit), College of Science & Technology, UTM ***International Campus***, Kuala Lumpur. Her current interests include information systems, IT outsourcing, system development and design, database, knowledge management, IS impact on organizations, adoption and diffusion of IT, computer ethics, computer Security, and information Security.