

# Computer Ethics: A Potent Weapon for Information Security Management

By Wanbil W. Lee, D.B.A., FBCS, FIMA, FHKIE, and Keith C.C. Chan, Ph.D.

Business corporations increasingly rely on their computer-based information systems to conduct themselves and make decisions. Executive management has urged these corporations to ensure a secure system, lest the data become vulnerable to unauthorized access and inappropriate disclosure (confidentiality of information), disruption or illegal utilization (availability of information), and improper modification (integrity of information). Decisions based on insecure and unreliable information can lead to disastrous consequences. Hence, information security is justifiable as a primary concern. However, a secure system not only depends on what the authorized actions and the authorized users require, but it is also viewed differently in different cultures such that how it is interpreted is “dictated by the individuals’ needs, customs and the law.”<sup>1</sup> Furthermore, enforcing confidentiality, upholding integrity and ensuring availability rely on the assumption of trust, provided to the required supporting services, that the data are correct and trustworthy and that any attempt to deny service may be atypical. Finally, ensuring a secure system requires a security policy and a security mechanism. Information security is the policy, and information security management is the mechanism.

## Information Security: Not Just a Hard Technical, but Also a Soft Legal/Ethical Concern

Information security must necessarily and sufficiently cover the technical, legal and ethical aspects of information security management, as abusing information systems is a technical issue as well as a management problem.<sup>2</sup> Information security management must also deal with technical as well as sociotechnical problems. That is, what makes up a secure system depends on what is required to carry out the authorized actions and satisfy the authorized users, and what is secure and authorized can be interpreted differently in different cultures, customs, corporate conventions and individual philosophical outlooks.<sup>3</sup>

It follows that the information security tools must be sufficiently diversified to handle the legal and ethical aspects, not just the technical aspects, of information security problems. As a result, physical and logical countermeasures, referred to as technical controls, have been implemented to handle the hard technical issues, and computer or cyberlaws,<sup>4</sup> computer or IT ethics,<sup>5</sup> or cyberethics<sup>6</sup> have been developed to deal with the soft legal and ethical/moral issues.

## The Argument

As technology advances, for example, the growth of the Internet, which has changed the rules for security,<sup>7</sup> and as hackers are always lurking to find a loophole somewhere, the existing 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, progress in 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 for information security management, it is argued that:

- There exists a relationship between computer ethics and information security
- It is necessary, but not sufficient, to trust people by setting a number of ethical rules. Education may help toward ethical awareness and action, such that computer ethics may actually, and not just theoretically, help information security management.

## Impact of Computer Ethics on Information Security

The relationship between information security and computer ethics does not look, on the surface, readily obvious, and even appears remote. It is, however, credible. Culture, customs, trust and privacy that characterize security fall within the realm of ethics. Computer ethics alert information security management to ethical considerations and warn potential offenders of ethical consequences in situations where the technical tools or the legal measures fail. In these cases, an ethical decision may be helpful in bringing about a solution. Furthermore, this conclusion is consistent with the following premises with respect to technical controls, computer laws and computer ethics:

- **Premise 1:** 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 difficult to trace. Quantifying the damage is problematic since the victims all too often withhold reporting the crime for reasons including fear of recrimination and bad publicity.<sup>8</sup> Therefore, the technical control tools are ineffective, with respect to legal issues.
- **Premise 2:** Computer laws have been enacted in various nations at an ever-increasing rate since the late 1980s, when

business and the society at large were forced to face the magnitude and severity of damage not experienced prior to computer crimes.<sup>9</sup> There has been a dramatic increase in specialized legislation to combat criminal behaviors related to computer crime, which include traditional crimes committed with the use of a computer and a variety of new, technology-specific criminal behaviors spawned by the rapid emergence of computer technologies and the exponential expansion of the Internet.<sup>10</sup> 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 no appropriate laws are found or the new law is too late for the case in hand. Hence, computer laws are at best a deterrent to computer crime, not a guardian of information.

• **Premise 3:** 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 individuals communicate with others.<sup>11</sup> 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 have promoted codes of ethical practice and even written these codes into their constitutions.<sup>12</sup> Notably, the Association for Computing Machinery (ACM) and the Institute of Electrical and Electronic Engineers—Computer Society (IEEE) developed in 1998 the *ACM/IEEE Software Engineering Code of Ethics and Professional Practice* in terms of eight principles:

1. For the public, software engineers shall act consistently with the public interest.
2. For the client and employer, software engineers shall act in a manner that is in the best interests of their clients and employer, consistent with the public interest.
3. Concerning the product, software engineers shall ensure that their products meet the highest professional standards possible.
4. With respect to judgment, software engineers shall maintain integrity and independence in their professional judgment.
5. About management, software engineering managers shall subscribe to and promote an ethical approach to the management of software development and maintenance.
6. For the profession, software engineers shall advance the integrity and reputation of the profession consistent with the public interest.
7. With colleagues, software engineers shall be fair to and supportive of their fellow workers.
8. About self, software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession.<sup>13</sup>

Guidelines for ethical practice are laid down by various international and national bodies, and these guidelines are similar in spirit and cover similar grounds, but may comprise

a different number of items and are composed of different wordings. The following are some international and national bodies' codes of ethics and writing on such codes:

- ISACA's *Code of Professional Ethics* guides the professional and personal conduct of members of the association and/or its certification holders.<sup>14</sup>
- ACM's *Code of Ethics*, the current version of which was adopted in 1992, specifies the rules and regulations under four major headings: general moral imperatives, more specific professional responsibilities, organizational leadership imperatives and compliance with the code.<sup>15</sup>
- The Japan Information Technology Service Industry Association's *Code of Ethics and Professional Conduct* is comprised of four components: relation to society, relation to clients, relation to fellow members and relation to employees.<sup>16</sup>
- The Hong Kong Computer Society's *Code of Ethics and Professional Conduct* covers professional competence and integrity, social implication, organization and leadership, and duty of profession.<sup>17</sup>
- The British Computer Society's *Code of Good Practice and Code of Conduct*<sup>18</sup>
- A series of ethical case studies issued by the Australian Computer Society<sup>19</sup>
- A comparison of more than 20 IT codes of ethics can be found in a book by Berleur and Brunnstein.<sup>20</sup>

While such codes may serve to deter potential offensive actions, they are limited because they rely on the moral obligation of the members; 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. Nonetheless, the codes of ethical professional conduct contribute to security because they do help reduce the incidence of abuse, fraud and software piracy, even though adoption of the codes cannot guarantee more ethical behavior.

It can arguably be concluded that, by inference from the results of analysis of the above codes, there exists a relationship between information security and computer ethics.

### **Effect of Ethical Rules and Education of Ethics**

A mini survey was conducted for a preliminary feel of the effect of ethics in the workplace and the role of education. The participants were part-time final year students for an undergraduate award in computing at Hong Kong Polytechnic University, ages ranging from early 20s to early 40s, in regular full-time positions in the computer industry, with titles ranging from help desk consultant to manager of 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 by students are fairly consistent between the 2006/07 cohort and the 2007/08 cohort. **Figure 1** summarizes the data obtained.

**Figure 1—Data From Survey**

Questions	Count of Positive Responses	
	2006/07	2007/08
Before attending the course:		
1.1 I had heard or was aware of computer ethics but I did not know if I carried out my work ethically.	5	8
1.2. I had never heard or was never aware of computer ethics, and I thought I carried out my work ethically	20	28
1.3. I had never heard or was never aware of computer ethics, and I was not sure if I carried out my work ethically.	46	54
After attending the course:		
2.1. I understand computer ethics, and I will conduct my work according to ethical principles.	51	64
2.2. I understand computer ethics, and I will not conduct my work according to ethical principles.	14	19
2.3. I have not changed my view because I do not fully understand the subject of computer ethics.	2	1
2.4. I have not changed my view because I do not subscribe to the subject of computer ethics.	1	1
2.5. I am indifferent because I do not care much whether my way of working is ethical or not.	3	5

Analysis of the data obtained indicates that:

- Before attending the course, the absolute majority of students claimed that they had never heard or were never aware of computer ethics, and less than 10 percent of these students claimed that they had heard or were aware of computer ethics.
- After attending the course, more than 90 percent of students claimed that they understood computer ethics. This clearly shows that there is an increase in students' awareness of computer ethics after attending the course, and supports the argument that education can play an effective role.

The data indicate that before attending the course, of the students who had never heard or were aware of computer ethics, more than 60 percent claimed that they were not sure if they carried out their work ethically and, conversely, about 30 percent claimed that they thought they carried out their work ethically. This appears to support the argument that proper introduction is necessary, thus confirming that teaching ethics is necessary. The response, by about 30 percent of students, a relatively significant number, reflects exactly a common phenomenon; when people are asked to explain why they think certain behavior or policy is wrong, they have difficulty articulating their reasons. When they express moral opinions, sometimes they are simply reacting as they think most people in their society react. Many who have strong moral beliefs have only a vague sense why the behavior is unfair or harmful. That is, people cannot give good reasons for believing what they do. This is why we need ethical analysis, and in turn, ethical theories.

The data also indicate that after attending the course, of the students who claimed that they understood computer ethics, 70 percent claimed to carry out their work according

to ethical rules but 20 percent ignored ethical principles in conducting their work. This supports the argument that ethical rules are necessary, but not sufficient.

## Conclusion

It can arguably be concluded, by inference from the previous arguments, that computer ethics has made its presence in the codes of professional conduct and that education has achieved some success, such that it supports the claim that computer ethics can be a potent weapon for information security management, because computer ethics actually, and not just theoretically, helps information security.

It is noteworthy that computer ethics is taught in computer science and computer engineering programs in various countries. For example, in the Hong Kong universities it is a compulsory course, particularly in those programs accredited by the Hong Kong Institution of Engineers for professional qualification.

However, further observation of the data obtained, as shown in **figure 1**, reveals that several stones have been left unturned, and thus several issues are raised. First, about 20 percent of those who had learned and claimed to understand computer ethics after attending the course planned to ignore the ethical principles in conducting their work. Why did these students still ignore ethical principles in their work and what are the possible factors that influence their behavior? Second, after attending the course about 1 percent of students claimed that they did not fully understand computer ethics, and another 1 percent claimed that they did not subscribe to computer ethics. Is effectiveness of teaching the subject the cause for this, and is there room for improvement, the small percentage notwithstanding? Third, 4-6 percent of students remained indifferent after attending the course. Is this a problem of impact (or lack of it) of the teaching? This culminates in the question of how and where that weapon can be made more effective, and leads to further investigation of specific issues, such as better promotion of professional codes of practice and provision of better teaching of the subject among other related issues.

It is hoped that this article and the authors' ongoing research will alert the computer security community, including information systems auditors, to the ethical practice of information security.

## Endnotes

- <sup>1</sup> Bishop, M. A.; *Introduction to Computer Security*, Addison Wesley, USA, 2005, p. 1
- <sup>2</sup> Aytes, K.; T. Connolly; "Computer Security and Risky Computing Practices: A Rational Choice Perspective," *Journal of Organizational and End User Computing*, July-September, vol. 16, iss. 3, 2004, p. 22-40
- <sup>3</sup> *Op cit.*, Bishop
- <sup>4</sup> For more information about the term "cyberlaw," see: Singh, Yatindra; *Cyber Laws: a Guide to Cyber Laws, Information Technology, Computer Software, Intellectual Property, 2<sup>nd</sup> Edition*, India, Universal Law Pub., 2005. Dudeja, V.D.; *Information Technology & Cyber Laws*, Ajay Verma for Commonwealth Publishers, India, 2001.

- <sup>5</sup> For an explanation of the term “IT ethics,” see: Northcutt, S.; *IT Ethics Handbook: Right & Wrong for IT Professionals*, Syngress Pub., USA, 2004.
- <sup>6</sup> For more information about the term “cyberethics,” see: Kizza, J.M.; *Computer Network Security & Cyber Ethics, 2<sup>nd</sup> Edition*, McFarlan, USA, 2006. Willard, N.E.; *The Cyber Ethics Reader*, McGraw-Hill, USA, 1997.
- <sup>7</sup> Bitpipe Inc., “Preemptive Protection: Changing the Rules of Internet Security: White Paper,” Internet Security Systems, 19 October 2004, [www.bitpipe.com/detail/RES/1083349267\\_979.html?src=mu.ij](http://www.bitpipe.com/detail/RES/1083349267_979.html?src=mu.ij)
- <sup>8</sup> Lee, W.W.; “A Deterrent Measure Against Computer Crime: Knowledge-Based Risk-Analytic Audit,” *Singapore Management Review*, January 1997, p. 19-45
- <sup>9</sup> Bainbridge, David; *Introduction to Computer Law, 5<sup>th</sup> Edition*, Pitman, UK, 2004
- <sup>10</sup> Ditzion, R.; E. Geddes; M. Rhodes; “Computer Crimes,” *The American Criminal Law Review*, vol. 40, iss. 2, 2003, p. 285-337
- <sup>11</sup> Maner, W.; “Unique Ethical Problems in Information Technology,” In: Hester, D.M; P.J. Ford; *Computers and Ethics in the Cyberspace*, Prentice-Hall, USA, 2001, p. 39-56
- <sup>12</sup> Cardinali, R.; “Reinforcing our Moral Vision: Examining the Relationship Between Unethical Behavior and Computer Crime,” *Work Study*, vol. 44, no. 8, November/December 1995, p. 11-17
- <sup>13</sup> Visit [www.acm.org/about/se-code](http://www.acm.org/about/se-code) for a detailed decryption of the elements that make up the eight principles.
- <sup>14</sup> ISACA, *Code of Professional Ethics*, [www.isaca.org/ethics](http://www.isaca.org/ethics)
- <sup>15</sup> Visit [www.acm.org/about/code-of-ethics](http://www.acm.org/about/code-of-ethics) for further details of the rules and regulations. See also: Anderson, R.; “The ACM Code of Ethics: History, Process, and Implications,” In: *Social Issues in Computing*, Huff, C.; T. Finholt; (Eds.), McGraw Hill, USA, 1994, p. 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).
- <sup>16</sup> [www.jisa.or.jp/en/introduction/ethics.html](http://www.jisa.or.jp/en/introduction/ethics.html)
- <sup>17</sup> [www.hkcs.org.hk/ethics.htm](http://www.hkcs.org.hk/ethics.htm)
- <sup>18</sup> [www.bcs.org/server/php?show=nav.6029](http://www.bcs.org/server/php?show=nav.6029)
- <sup>19</sup> [www.acs.org.au/index.cfm?action=list&groID=casestudy](http://www.acs.org.au/index.cfm?action=list&groID=casestudy)
- <sup>20</sup> Berleur, J.; K. Brunnstein, K.; *Ethics of Computing: Codes, Spaces for Discussion and Law*, Springer Verlag, 1996

**Wanbil W. Lee, D.B.A., FBCS, FIMA, FHKIE**

is honorary research associate at the Centre of Information Security & Cryptography of The University of Hong Kong, and visiting lecturer in IT professionalism and ethics in the Department of Computing of The Hong Kong Polytechnic University. His field is information systems, which is grounded in the domains of mathematics, operations research, expert systems, management and auditing. His current research interests include information security management and computer ethics. He sits on a number of committees and boards, and has been the director of education for the ISACA Hong Kong Chapter for 12 years. He can be reached at [wanbil@acm.org](mailto:wanbil@acm.org).

**Keith C.C. Chan, Ph.D.**

is professor and head of the Department of Computing at The Hong Kong Polytechnic University. Prior to this post, he worked on development of multimedia and software engineering tools at the IBM Canada Laboratory. Chan’s research interests are in the areas of software engineering and data mining. He has been a consultant to government agencies and large and small-to-medium-sized companies in China, Hong Kong, Italy, Malaysia and Singapore. He can be reached at [cscchan@comp.polyu.edu.hk](mailto:cscchan@comp.polyu.edu.hk).