# Reinforcing our moral vision: examining the relationship between unethical behaviour and computer crime

*Richard Cardinali*

## Introduction

According to Senn[1] few areas of social behaviour are as complex and controversial as ethics. Philosophers have been debating ethics for the past 3,000 years without arriving at a consensus. But that is the good news. The bad news is that everyday we witness grossly unethical behaviour on the part of a few government officials and corporate executives, some of whom even seem to take pride in their schemes. Many of the people involved get away with their unethical behaviour[1].

Information systems embody all computerized systems associated with gathering, processing and disseminating information. These systems are generally found on all organization computers, and as computers become more user-friendly, computer crime and unethical behaviour appear to escalate. Compared to the early years in the field when few people in business truly understood the complex nature of computers, today we find knowledgeable end users with access to a wide variety of systems. Therefore, the potential for misuse becomes widespread. No company seems to be completely safe from the abuse and it is being discovered that physical security alone will not solve the problem.

Ethics generally refers to conduct concerning right and wrong. Since ethics deals with conduct and corporate decision making is inherently based on the conduct of the decision makers. It is safe to assume that ethical or unethical behaviour is part of the corporate environment. Furthermore, since information systems are a major part of the corporate decision-making process, ethics and information systems are very likely an integral part of corporate America. Thus the relationship between ethics, crime and information systems can be examined[2].

The author acknowledges research assistance by Eric Waldman, Management Information Major, Central Connecticut State University, New Britain, Connecticut, USA.

## Types of unethical behaviour

Today society is marked by contrasting behaviour. Unethical behaviour exists at all levels of society from government to street crime. Managers cannot expect different behaviour from systems professionals. One device the manager has is to understand what motivates people to behave in an unethical manner and manage the situation without expecting it to disappear. The successful manager can create an environment which will promote ethical behaviour.

### *Invasion of privacy*

There are a number of identifiable unethical behaviours. Invasion of privacy is one type of unethical behaviour which takes place every day in business. For example, insurance company employees can view any client's medical history. Often the files are read as a matter of curiosity rather than official business. There have been cases where confidential file materials have been shared with non-company personnel. After checking a medical history and discovering something unknown to anyone else the next logical action for an unethical employee would be to make the information public.

Another common privacy invasion is to sell customer information. This form of invading your privacy is to sell mailing lists. Many companies routinely sell information without customer permission. Companies record this information when someone reacts to a product rebate or completes a registration or warranty card. Often the information required – age, sex, income – has nothing to do with the product or the warranty.

In other cases of unethical behaviour, a data entry person can alter information. For example, a data entry clerk for a credit company may be required to enter information on someone he or she knows and for some reason dislikes. That clerk can intentionally enter incorrect information resulting in that person receiving a bad credit rating. When that person applies for credit he or she will be refused because of the incorrect data entry. At this point it is up the person refused credit to try to discover the error and prove that it is in fact an error. This process could take months.

### *Embezzlement*

Embezzlement is a serious computer crime. People usually engage in embezzling for a number of reasons. The most common is because they wish to live beyond their means. There may be other reasons but most of the time it is simply extravagant living. Embezzlers are difficult to discover. For example, the stereotypical white collar criminal is usually a middle-class white male between the ages of 18 and 30. The management is least likely to suspect such a person[3]. Typically, it could be an application programmer who knows the weakness of the computer system and often feels he has been treated unfairly. Usually the motive is financial gain and seeking revenge on the organization or a specific person in the organization. Employee screening efforts are often ineffective since computer criminals usually have the characteristics most employers are seeking[4].

### *Hackers*

Hackers are unauthorized but talented computer people. They usually have no

criminal intent but merely enjoy the challenge of breaking into a company's computer system[5]. All hackers require is a phone number and a randomly generated password. After entering a corporation's computer it is possible for information to be changed or eliminated. Companies are focusing on how to guard against outside invaders. Advances in information technology make it easier to collect, store and disseminate personal information. "It is hardly a stretch of the imagination to envision how government and private organizations can monitor a person's life by linking into a worldwide computer network"[6].

A recent study demonstrates the magnitude of hacker interference. Security breaches by a group of hackers called "Masters of Destruction" cost Southern Bell Telephone Company $370,000 including the cost of locating the hackers[7]. Other cases include exploitation and unauthorized dispersion of software by hackers who "pirate" programs illegally.

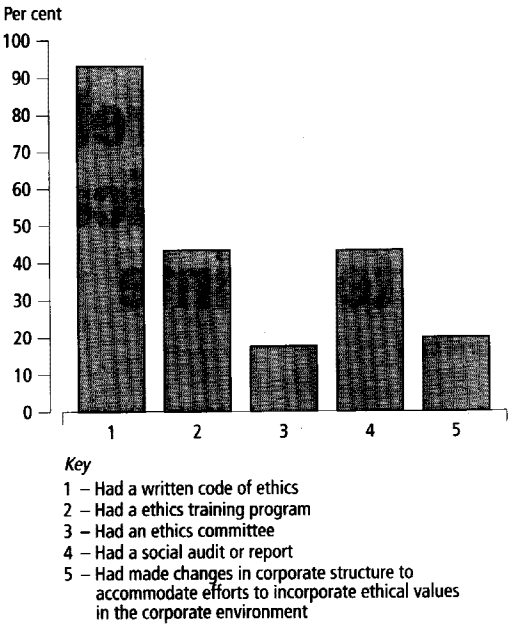
***Viruses***

Natural disasters and direct attacks by humans are not the only threats to computer systems. "Infectious" programs called viruses are far more insidious foes, because they infect the computer and cause damage without the user's knowledge. Often an innocuous screen message such as "Gotcha" is the user's only clue that something has gone awry. The potential damage can be as serious as the loss of the entire contents of a disk.

A computer virus is the latest refinement of a type of rogue program which has been present for at least 20 years. Known also as the Trojan Horse or the Logic Bomb, this type of program damages or destroys data or programs. Computer viruses have two insidious characteristics: first, they appear to be introduced to an organization by an outside agent and, second, they are designed to replicate themselves many times. But all is not lost! "Vaccine" programs are available which detect and delete your intruder. However, these must be used with care because viruses have been known to exist in vaccine programs[8].

## Management ethics

Management must strive to establish an ethical standard of conduct. A study by the Center for Business Ethics at Bentley College demonstrates that most organizations do not have an established standard of conduct (Figure 1). Once a foundation has been established with usable standards of conduct, the next step is to integrate it through the management process by creating a working environment where ethical behaviour is maximized. Perhaps the most important issue would be for management to act as role models. The management should avoid sending mixed messages. Witnessing unethical acts by upper management promotes identical behaviour from the employees. Additionally, at a time when large companies are reducing their workforce (downsizing), overburdening workloads for existing employees are becoming common. Managers must ensure that there is an equitable distribution of the workload. This will prevent employees from becoming discouraged and heighten the opportunity for unethical or criminal behaviour. For example, Crino and Leap[9] state that a feeling of powerlessness and mistreatment are important factors for unethical behaviour. From a manager's viewpoint, creating a team environment will help employees feel they indeed have power and are part of the decision-making process.




*Source*: 1984 study by the Centre for Business Ethics at Bentley College

Figure 1. 1984 study by the Center for Business Ethics at Bentley College, with a response rate of 27 per cent

## Ways of deterring unethical behaviour

There really is no fool proof way of preventing unethical behaviour in the information systems field. The focus for information professionals is to try to deter unethical behaviour. Several methods are recommended. State and federal legislation, the use of safeguards, the use of a written code of ethics and punctual action taken against unethical behaviour. These are but a few of the methodologies available and will be discussed in the next section.

***Legislation***

To date, laws enacted by the Federal Government concerning computer crimes, have not been fully effective. Most of the legislation has been concerned with privacy. For example, the Federal Privacy Act regulates the collection and use of personal data. The law specifies that individuals have the right to inspect their personal records, make copies, and correct or remove erroneous or misleading information. The reason for this minimal course of action is due to several factors. "First, many people feel that computer crime is not a special or exotic type of

crime"[10] which can be covered by existing laws like patents, copyrights, fraud and embezzlement which are all illegal whether relating to computers or not. "Second, others believe the new state laws will be sufficient to handle the problems"[10]. Florida was the first state to pass a computer crime bill back in 1978. Since then more than 18 states have followed Florida's lead. "Finally, [there is] the difficulty in wording new legislation in a way that will keep pace with computer technology"[10].

The following is a partial list of legislation passed in the USA which can promote ethical behaviour and assist in diminishing computer crime.

- Fair Credit Reporting Act of 1976 – allows individuals to have access to and challenge credit reports.
- Freedom of Information Act of 1970 – gives individuals access to data gathered by federal agencies pertaining to themselves.
- Electronic Funds Transfer Act of 1982 – requires institutions to provide their patrons with a statement of their rights under the federal law.
- Computer Fraud and Abuse Act of 1984 – "Defines certain crimes against Federal databases. These include certain actions of outsiders attempting access to an automated information system via a dial-in line"[11].
- Electronic Communication Privacy Act and Computer Fraud and Abuse Act 1986 – federal laws prohibit intercepting data communication messages, stealing and destroying data, or trespassing in federal government related computer systems.
- Computer Matching and Privacy Act 1988 – regulates the matching of data held on federal agency files to verify eligibility for federal programs[12].

"The legal systems provide for rights and obligations and methods of enforcing these rights or obligations"[13]. These laws are only enacted after a breech of security has occurred, therefore the legislation is held as a deterrent to computer crime. Individually each organization must take measures to prevent the crime. There is no doubt that computer crime laws play a beneficial part in organizations fighting computer crime. These laws acknowledge that recently accepted questionable behaviour is now in fact an offence. The laws also promote information management to establish more clearly what constitutes authorized and unauthorized behaviour.

***Safeguards***

The vulnerability of information systems has been the subject of debate in government agencies for a number of years. Recently an experimental "clipper chip" would allow government agencies into the files of private corporations worldwide. Government would mandate that these chips be installed in all computers manufactured in the USA. As a measure of protection, government officials claimed that a two-part access code would be required. Each part of the code would be available only when necessary. Corporate leaders viewed this practice with great reservation and the project did not materialize.

> *"The effects of computer crime on businesses can be catastrophic"*

Companies today are trying to do everything possible to prevent unethical behaviour from interfering with their operations. The effects of computer crime on businesses can be catastrophic, databases may be changed, information lost or deleted. Companies, therefore, must employ safeguards to prevent all forms of computer crime.

Several methods to prevent computer crime are suggested. The placement of terminals in secure areas is one basic way to prevent systems manipulation. This can be accomplished by using security cameras in the computer areas to monitor those attempting to access information. If an attempt is made, security personnel identify and apprehend the person. Securing the terminals in a restricted access room may also assist.

In the past hackers have been known to call a company pretending to be an employee. Those answering the phone will normally give out information thinking they are helping a fellow employee. This practice has led to written policies and procedures for handling this type of situation. One simple procedure is to have the person answering the phone call the supervisor and ask the supervisor to verify the identity of the caller. The supervisor, recognizing the subordinate's voice, gets in touch with the systems department who calls the person back to verify the identity of the caller. If the hacker called the systems supervisor directly with no call back, the person in the systems department would have no way of knowing who was really on the other end.

Another method of safeguarding information is through an effective password system. A password is a key, it opens your door to the system. Theoretically, if you have kept your password a secret, no-one can access your account. Most systems cut off access after entering the wrong password several times. This feature is particularly good for hackers or unauthorized personnel trying a number of possible combinations. To be effective, employees must change their passwords often. How often is determined by the organization's security officer. This prevents access by people who discover the previous password. Most organizations print lists which show every log-on or attempted log-on.

Batch control has become an effective follow-on to effective password control. It is especially effective to detect if data has been manipulated in any way. This is accomplished by the computer. It "totals the transactions going into the computer and then totals the processed results"[14]. If the totals match, no problem exists, but if they do not the data has been changed illegally. It also may be an early indication that future data problems may arise and precautionary measures should be taken. This appears to be one of the simplest way to control the integrity of information. Additionally, using range checks and checking reasonableness can be incorporated into ways of checking the correctness of data entry. These checks are accomplished at the point of data entry. The computer examines the input data and ensures the information is reasonable (i.e. the weekly salary may be between $200

and $1000, if the data entered in this field falls within this range it is acceptable). If the data is not reasonable a flag will immediately signify a problem with the data.

Parity checks are also excellent for detecting input errors. In this methodology an additional bit is added to each byte. All the bits are added up and depending on even or odd parity, the check bit is turned on or off. This ensures the data being sent is the same as the information being received. This technique greatly enhances data integrity.

There are a number of other procedures. For example, the use of encryption and decryption devices is one of the more complicated methods of stopping unwanted persons from acquiring and understanding illegally obtained data. An encryption device is used to scramble information during the transmission of data from one computer to another. The receiving computer must be equipped with a decryption device to decode the information. This process also helps to ensure the information has not been manipulated during data transmission.

The rise in the importance of computer security has generated a need for a specialist in security matters. Whether or not a company actually has an information security administrator, security awareness must start with top management. A security policy is useless if it is not fully supported by top management. Security is not the sole responsibility of security personnel, but of the entire organization. The concept, according to Forcht[8], of shared security must be promoted by all levels of management to have a successful security system.

### *Software*

The increased use of computers and the computer literacy level of users have heightened public awareness of the sensitive nature of information which is processed and stored in a computer. In a collaborative effort in 1991, the System Security Study Commission, the Computer Science and Telecommunications Board, the Commission on Physical Science, Mathematics and Applications and the National Research Council offered definitive guidelines on system and software security measures. The generally accepted system security principles for computer systems presented the idea that "it is possible to enunciate a basic set of security related principles that are so broadly applicable and effective for the design and use of systems that they ought to be part of any operational requirements"[8]. There are also a number of software packages which assist in preventing unauthorized activity, accidental erasing of files and uses a master key system. Table I previews several of these programs and highlights their security features.

### *Codes of ethical behaviour*

Many companies currently do not have a written code of ethics. As the information systems field grows a greater number of organizations are adopting them into their policy and procedure manuals. They are being used as guidelines for their employees to follow even though they are "seldom enforced or even remembered"[16].

In developing a code of ethics, five guidelines are suggested:

(1) Inspirational – it should inspire ethical conduct.

(2) Sensitivity – it should point out moral aspects of the work.

(3) Disciplinary – it should state and enforce rules of professionalism.

(4) Advising – it should guide employees through questionable activities.

(5) Awareness – it should alert prospective clients and employees to what they may or may not expect by way of service from a member of the profession.

Three other factors which should be considered are[2]:

(1) Certification – "an affirmation by a government or private organiza-

| | Software/ hardware based | Hard disk | Audit trail | Custom menu | Password management | Auto propriety | FED[a] DES[b] | Master key |
|---|---|---|---|---|---|---|---|---|
| Watchdog (Fischer International Systems, Naples, Florida) | Software | Required | Yes | No | Yes | Yes | No | No |
| Protec (Sophco, Boulder, Colorado) | Software | Required | Yes | Yes | Yes | Yes | Yes | No |
| Secure!/ Secure! PS (Winterhalter, Ann Michigan) | Either | Optional | Yes | No | No | Yes | Yes | Yes |
| PC/DACS (Pyramid Development, West Hartford, Connecticut) | Software | Required | Yes | Yes | Yes | Yes | No | Yes |

*Key*:
[a]FED = automatic file encryption/decryption
[b]DES = data encryption standard
*Source*:[15]

Table I. Security software packages

tion that an individual has met certain qualifications".

(2) Licensing – "The administrative lifting of a legislative prohibition".

(3) Accreditation – "an affirmation by a governmental or private organization that an educational institution meets certain standards".

Business organizations are not alone in the development of ethics codes. Several associations currently have a written code of ethics accompanying a standard of conduct. For example, the Association for Computing Machinery (ACM) Professional Conduct and Procedure for the Enforcement of the ACM code of Professional Conduct; British Computer Society (BCS) Code of Ethics; and Data Processing Management Association (DPMA) Code of Ethics and Standards are a few professional associations which developed an ethics code. Other societies that have a written standard of ethics are Certified Systems Professional (CSP), and the Canadian Information Processing Society (CIPS). An example of a code of ethics and standards of conduct for DPMA is provided:

Code of ethics
I acknowledge:

- That I have an obligation to management, therefore I shall promote the understanding of information processing methods and procedures to management using every resource at my command.
- That I have an obligation to my fellow members, therefore, I shall uphold the high ideals of DPMA as outlined in its international bylaws. Further, I shall cooperate with my fellow members and shall treat them with honesty and respect at all times.
- That I have an obligation to society and will participate to the best of my ability in the dissemination of knowledge pertaining to the general development and understanding of information processing. Further, I shall not use knowledge of a confidential nature to further my personal interest, nor shall I violate the privacy and confidentiality of information entrusted to me or to which I may gain access.
- That I have an obligation to my employer whose trust I hold, therefore, I shall endeavor to discharge this obligation to the best of my ability, to guard my employer's interests, and to advise him or her wisely and honestly.
- That I have an obligation to my country, therefore, in my personal, business and social contacts, I shall uphold my nation and shall honor the chosen way of life of my fellow citizens.
- I accept these obligations as a personal responsibility and as a member of this association. I shall actively discharge these obligations and I dedicate myself to that end.

***Standards of conduct***

These standards expand on the Code of Ethics by providing specific statements of behaviour in support of each element of the code. They are not objectives to be strived for, they are rules which no true professional will violate. It is first of all expected that information processing professionals will abide by the appropriate laws of their country and community. The following standards address tenets that apply to the profession[10].

The code also lists the employees' obligations to management, fellow members of the profession, society and the employer. Unlike other professions such as accounting, law or medicine, the information field is still young and perhaps additional time is needed to develop standards fully. One important reason for professional bodies to develop recognizable standards is the quality of performance that it assures.

> In a fast growing set of disciplines such as the information processing industry, the ability to show the consumers of information processing services that one has satisfied certain minimum standards is often a commercial advantage[13].

## Enforcement

A code of conduct will only be taken seriously if it is enforced consistently. Companies will not prosecute individuals for computer crime. They often feel that the publicity will hurt their image. They often quietly suspend the individual. This could create an environment in which such acts are considered acceptable because there is no punishment. The problem is never solved this way because those involved will likely find another position and continue with their unethical and illegal behaviour.

Management must establish guidelines to ensure the code violators are punished. It was noted by Coleman[17] that in comparison to street criminals, the treatment of white collar criminals presents a double standard in the criminal justice system. White collar criminals are far less likely to be arrested, and even when arrested, they typically receive a much lighter sentence than their street crime counterparts.

## Can ethics be taught?

Many doubt whether ethics can be taught. Lester Thurow said:

> If they haven't been taught ethics by their families, their clergymen, their elementary school and secondary schools, their liberal arts college or engineering schools or business firms where most of them have already worked prior to getting a business degree, there is very little we can do[18].

While Kirk Hanson said:

> In ethics we hope to become one or more positive influence on their values...we can help prepare the "good MBAs" to manage the strength of their own characters, to deal effectively with predictable ethical challenges in any business career[18].

Still Hosmer stated:

> Maybe you cannot change moral standards. But you can teach people how to analyse questions so as to bring to bear whatever moral standards they have[18].

There is little evidence to prove or disprove either side of this controversy. One study by D.M. Maltb in 1988 shows that business majors have lower ethical values when it comes to questionable business practices than do other students. His study "showed that the majority of respondents who had formal ethics training believed that the training had been 'very successful' by enabling them to identify value conflicts (81.9 percent)"[18].

In other studies it seems that ethical behaviour is more prevalent in companies that take a strong ethical stand and enforce ethical employee behaviour[19].

Captains of industry feel ethics should not be legislated but rounded on the principle of self-control and performance. This has brought increasing interest in teaching business ethics in recent years. Harvard, MIT and Georgia Tech., to mention a few, have all adopted ethics programmes in their curricula.

Ethical behaviour is found to have a direct link to moral development. Researchers also noticed one cannot measure directly ethical behaviour and the effect on people in a classroom. Thus, a correlation between ethical behaviour and moral development is critical to measure any change in ethical behaviour. A defining issues test

(DIT), developed by Rust[20], measures moral development. Six questions relating to morals are asked to implement this test. These results are then used to determine if there has been any improvement in moral behaviour.

Rest and Thoma[21] have reviewed 55 studies, all of which have used the defining issues test, to study moral development. These results showed 25 studies to have had positive results. Their study shows age has a large influence on the results of the tests. Jones points out that: "Adult subjects responded best to treatment, followed by college students, senior high school students, and finally, junior high school students"[22].

Studies have shown that ethics can be "taught under conditions which are highly conducive to advances in moral development"[22]. Students who choose voluntarily to take an ethics class in business showed significant improvements in moral development, while students who were required to take the course as part of their curriculum showed less improvement in their moral development. This shows you cannot teach ethics to someone who does not have any desire to learn[23]. However, in order to stop morals from declining, it may be a good idea.

## Ethical beliefs of MIS professionals

Most people in the management information systems (MIS) field feel that they and others have a number of opportunities to engage in unethical behaviour. These people also feel most MIS professionals do not act unethically. Further, they believe that one does not have to be unethical to be successful. Another factor considered by MIS professionals is that the field is young compared to that in other established professions. Because information is such an important area which impacts on comparing success, professionals must ensure that its members are both professional and ethical.

## Philosophies

Ethical beliefs can be classified into two philosophies, or a combination of deontological and teleological perspectives. Deontologists feel certain features of an act make that particular act right or wrong. For example, it is wrong to give or receive a bribe regardless of the circumstances. While on the other hand a teleologist will focus on the consequences of an action. So if one can achieve more good from giving a bribe the act will be acceptable. The majority of people have some combination of the two. This falls in line with the fact that most philosophers recognize a mixed deontological-teleological system of ethics[24].

A study of 61 MIS professionals, was completed by Vitell and Davis[25]. The results demonstrated these professionals believe their firms have high ethical standards. When the authors address firms having high ethical standards they are referring to top management. Of the respondents, 80 per cent felt that their managers did not engage in unethical practices, while 73 per cent said it was not necessary to take part in unethical behaviour to be successful. This demonstrates that there may be little or no pressure to behave unethically to succeed, since most respondents felt that their superiors did not have to compromise their ethics. Other results showed the majority of MIS professionals felt their corporations had a social responsibility to the public in addition to a responsibility to shareholders. These results are consistent with the belief that their managers are ethical.

*"There are many opportunities to behave unethically"*

Most people in the MIS field feel there are many opportunities to behave unethically. They also believe their superiors engage in and encourage ethical behaviour. Since "top management is perceived as supporting ethical behaviour, then individuals are more optimistic about the link between success and ethical behaviour"[25], and thus less likely to compromise their own personal ethical beliefs.

## Conclusion

Initiating security countermeasures in an information system or in an organization is a complex process involving many steps. It is more involved than simply insisting on ethical behaviour of employees. It involves an understanding of human behaviour, how people act and why they act as they do[26]. Some firms use people-oriented controls to try to prevent unethical behaviour. These controls include careful screening of all applicants, detailed checking of references and, when possible, checking of credit histories. They also bond employees. Yet unless organizations enforce punishment of unethical or criminal employees, the screening will be ineffective.

With a combination of actions from top management and the codes being written by professional bodies, MIS professionals are optimistic about the link between success and ethical behaviour. As business end users, we have a responsibility to do something about some of the abuses of information technology in the workplace. When we are successful in developing an ethical environment, it will have an effect on those around us. Even though the information systems field is relatively young, it is well on its way to having standards which equal or surpass the more mature fields.

It then becomes important for all of us to understand the ethical dimensions of working in business and using information technology[4]. As a future managerial end user or seasoned information professional, the responsibility to make decisions about business activities and the use of information technology will always have an ethical dimension that must be considered[27].

Understanding human motivation and the relationship to computer crime is a difficult task. In an environment of rapidly changing technology, a struggle often exists between power, profit and social values. Generally people are ethical, but computers can create temptation which many may find irresistible. Employee motivation, training and awareness become critical in controlling business information resources during this fast-paced electronic age.

### Notes and references

1. Senn, J., *Information Technology in Business*, Prentice-Hall, Englewood Cliffs, NJ, 1994.

2. Dejoie, R., Fowler, G. and Paradice, D., *Ethical Issues in Information Systems*, Boyd & Foster, Boston, MA, 1991.
3. Mizock, M., "Ethics – the guiding light of professionalism", *Data Management*, August 1986, Vol. 24 No. 8, pp. 16-18, 29.
4. Schweitzer, J., *Computer Crime and Business Information: A Practical Guide for Managers*, Elsevier Publishing, New York, NY, 1986
5. The National Center for Computer Data and RGC Associates in Michael Alexander's "Hacker Stereotypes Changing", *Computer World*, April 1989, claims that 36 per cent of computer crimes involve theft of money, while 34 per cent cite theft of services, the remaining 30 per cent consists of theft of information 12 per cent, data alteration 8 per cent, and others 10 per cent.
6. Agranaoff, M.H., "Controlling the threat to personal privacy: corporate policies must be created", *The Journal of Information Systems Management*, Vol. 8 No. 3, Summer 1991, pp. 48-52.
7. Hoffman, L., *Modern Methods for Computer Security and Privacy*, Prentice-Hall, Englewood Cliffs, NJ, 1990.
8. Forcht, K.A., *Computer Society Management*, Boyd and Fisher, New York, NY, 1994.
9. Crino, M.D. and Leap, T.L., "What HR managers must know about employee sabotage", *Personnel*, Vol. 66 No. 5, May 1989.
10. Athey, T.H. and Zmud, R.W., *Computers and Information Systems*, Scott, Foresman and Company, Glenview, IL, 1986.
11. Abrams, M.D. and Podell, H.J., *Tutorial Computers and Network Security*, IEEE Computer Society Press, Washington, DC, 1987.
12. O'Brien, J.A., *Information Systems*, Irwin Company, Boston, MA, 1994.
13. Fites, P.E., Kartz, M.P.J. and Bredner, A.F., *Control and Security of Computer Information Systems*, Computer Science Press Inc., Rockville, MD, 1989.
14. Behling, R., *Computers and Information Processing*, Kent, Boston, MA, 1986.
15. Johnson, R.E., "The macro community matures", *Infosystems*, 2 February, 1988, p. 34.
16. Clarke, R., "Economic, legal, and social implications of information technology, *MIS Quarterly*, Vol. 12 No. 4, December 1988,pp. 517-20.
17. Coleman, J.W., *The Criminal Elite: The Sociology of White Collar Crime*, St Martin's Press, New York, NY, 1990
18. Kohls, J., Chapman, C. and Mathieu, L., "Ethics training programs in Fortune 500 companies", *Business & Professional Ethics Journal*, Vol. 8 No. 2, Summer 1989, pp. 73-88.
19. Laczniak, G. and Inderrieden, E.J., "The influences of stated organizational concerns upon ethical decision making", *Journal of Business Ethics*, Vol. 6 No. 4, 1987, pp. 297-307.
20. Rust, J.R., *Development in Judgement Moral Issues*, University of Minnesota Press, Minneapolis, MN, 1979.
21. Rust, J.R. and Thoma, S.J., *Moral Development*, Praeger, New York, NY, 1986.
22. Jones, T.M., "Can business ethics be taught? Empirical evidence", *Business & Professional Ethics Journal*, Summer 1989, pp. 73-88.
23. A review of the literature reveals several arguments which contend the answer to the prevention of unethical behaviour and the resulting computer crime lies in educating those who enter the MIS profession. It is argued that the emphasis in college curricula tends to be on the technical side and that ethics courses should be required.
24. Hunt, S.D. and Vitell, S., "A general theory of marketing ethics", *Journal of Macromarketing*, Vol. 6 No. 1, Spring 1986, pp. 5-46.
25. Vitell, S.J. and Davis, D.L., "Ethical beliefs of MIS professionals: the frequency and opportunity for unethical behavior", *Journal of Business Ethics*, January-June 1990, pp. 63-70.
26. The views of Lawrence Kohlberg shed some light on how a person's ability to reason about moral matters is developed. According to Kohlberg, our ethical make up begins when we are children and progresses through adulthood until our beliefs are developed.
27. Cougar, D.J., "Preparing IS students to deal with ethical issues", *MIS Quarterly*, Vol. 13 No. 2, June 1989.

**Further reading**

Adams, D.R., Wagner, G.E. and Boyer, T.J., *Computer Information Systems: an Introduction*, Southwestern Publishing Co., Cincinnati, OH, 1983.

Capron, H.L., *Computers, Tools for Information Age*, Benjamin-Cummings, Menlo Park, CA, 1987.

Gemignani, M.C., *Advances in computers*, Academic Press Inc., Vol. 22, 1983, pp. 24-6.

Hsiao, D.K., Kerr, D.S. and Madnick, S.E., *Computer Security*, Academic Press, New York, NY, 1979.

Richard Cardinali in Associate Professor in the Management Information Systems Department at Central Connecticut State University, New Britain, USA.