Ethics in information technology

From The Computer Ethics Institute

1. Thou shall not use a computer to harm other people.
2. Thou shall not interfere with other people’s computer work.
3. Thou shall not snoop around in other people’s computer files.
4. Thou shall not use a computer to steal.
5. Thou shall not use a computer to bear false witness.
6. Thou shall not copy or use proprietary software for which you have not paid.
7. Thou shall not use other people’s computer resources without authorization or proper compensation.
8. Thou shall not appropriate other people’s intellectual output.
9. Thou shall think about the social consequences of the program you are writing or the system you are designing.
10. Thou shall always use a computer in ways that ensure consideration and respect for your fellow human of A study published in 1999 examined computer use ethics of eight nations: Singapore, Hong Kong, the United States, England, Australia, Sweden, Wales, and the Netherlands.
11. This study selected a number of computer-use vignettes (see the Offline titled The Use of Scenarios in Computer Ethics Studies) and presented them to students in universities in these eight nations.

This study did not categorize or classify the responses as ethical or unethical. Instead, the responses only indicated a degree of ethical sensitivity or knowledge about the performance of the individuals in the short case studies. The scenarios were grouped into three categories of ethical computer use: software license infringement, illicit use, and misuse of corporate resources. These were the findings: Software License Infringement The topic of software license infringement, or piracy, is routinely covered by the popular press.

Among study participants, attitudes toward piracy were generally similar; however, participants from the United States and the Netherlands showed statistically significant differences in attitudes from the overall group. Participants from the United States were significantly less tolerant of piracy, while those from the Netherlands were significantly more permissive. Although other studies have reported that the Pacific Rim countries of Singapore and Hong Kong are those countries to be moderate, as were attitudes in England, Wales, Australia, and Sweden.

This could mean that the individuals surveyed understood what software license infringement was, but felt either that their use was not piracy, or that their society permitted this piracy in some way. Peer pressure, the lack of legal disincentives, the lack of punitive measures, and number of other reasons could a explain why users in these alleged piracy centers disregarded intellectual property laws despite their professed attitudes toward them. Even though participants from the Netherlands displayed a more permissive attitude toward piracy, that country only ranked third in piracy rates of the nations surveyed in this study.

Illicit Use The study respondents unilaterally condemned viruses, hacking, and other arms of system abuse. There were, however, different degrees of tolerance for such activities among the groups. Students from Singapore and

Hong Kong proved to be significantly more tolerant than those from the United States, Wales, England, and Australia. Students from Sweden and the Netherlands were also significantly more tolerant than those from Wales and Australia, but significantly less tolerant than those from Hong Kong.

The low overall degree of tolerance for illicit system use may be a function of the easy correspondence between the common crimes of breaking ND entering, trespassing, theft, and destruction of property and their computer-related counterparts. Misuse of Corporate Resources The scenarios used to examine the levels of tolerance for misuse of corporate resources each presented a different degree of non-company use of corporate assets without specifying the company’s policy on personal use of company resources.

In general, individuals displayed a rather lenient view of personal use of company equipment. Only students from Singapore and Hong Kong view personal use of company equipment as unethical. There were several absentia differences in this category, with students from the Netherlands revealing the most lenient views. With the exceptions of those from Singapore and Hong Kong, it is apparent that many people, regardless of cultural background, believe that unless an organization explicitly forbids personal use of its computing resources, such use is acceptable.

It is interesting to note that only participants among the two Asian samples, Singapore and Hong Kong, reported generally intolerant attitudes toward personal use of organizational computing resources. The reasons behind this are unknown. Ethics and Education Attitudes toward the ethics of computer use are affected by many factors other than nationality. Differences are found among individuals within the same country, within the same social class, and within the same company. Key studies reveal that the overriding factor in leveling the ethical perceptions within a small population is education.

Employees must be trained and kept aware of a number of topics related to information security, not the least of which are the expected behaviors of an ethical employee. This is especially important in information security, as many behavior is unethical or even illegal. Proper ethical and legal training is vital to creating an informed, well prepared, and low-risk system user. Deterring Unethical and Illegal Behavior There are three general causes of unethical and illegal behavior: Ignorance? Ignorance of the law is no excuse; however, ignorance of policy and procedures is.

The first method of deterrence is education. This is accomplished by means of designing, publishing, and disseminating organization policies and relevant laws, and also obtaining agreement to comply with these policies and laws from all members of he organization. Reminders, training, and awareness programs keep the policy information in front of the individual and thus better support retention and compliance. Accident? landfills with authorization and privileges to manage information within the organization are most likely to cause harm or damage by accident.

Careful planning and control helps prevent accidental modification to systems and data. Intent? criminal or unethical intent goes to the state of mind of the person performing the act; it is often necessary to establish criminal intent to successfully prosecute offenders. Protecting a system against those with intent to cause harm or damage is best accomplished by means of technical controls, and vigorous litigation or prosecution if these controls fail.

Whatever the cause of illegal, immoral, or unethical behavior, one thing is certain: it is the responsibility of information security personnel to do everything in their power to deter these acts and to use policy, education and training, and technology to protect information and systems. Many security professionals understand the technology aspect of protection but underestimate the value of policy. However, laws and policies and their associated penalties only deter if three conditions are present: Fear of penalty? Potential offenders must fear the penalty.