ABSTRACT. This article discusses the role of ethics as it relates to a student computer lab in a college setting. The use of the computer as a necessity for education provides the background for a sample case study involving a breach of ethical conduct. The technical and administrative solutions to the sample case are described. Proposed solutions to prevent future breaches of ethical conduct are presented along with justification for the proposed solutions.

Introduction

The computer has become such an integral part of life in general that students in a college environment expect and demand extensive access to computers. Indeed, the concept of a student becoming “computer literate” is endemic to a fundamental college education. It is therefore imperative that a college provide students with a wide variety of computer experiences. These experiences can be in the form of formal academic courses that teach concepts and skills in computing topics ranging from word processing software to programming to Computer Aided Drafting. On the other hand, computer experiences can be available in the form of “open” labs that allow students freedom to access library holdings and course-specific software. From an even broader perspective, students need to be able to use campus computers to access information that is beyond the physical setting of the campus. Indeed, with the advent of the “Information Superhighway”, student access to Internet will be an essential part of learning process. Consequently, it is expected that a college computer lab provide all the facilities necessary to provide for a broad base of learning experiences.

“There are four distinct types of users on most campuses; students, faculty, administration, and classroom/lab facilities” (Wasch, 1992). A typical college might have several open labs that are primarily designated for student use. At any given time these labs may have Computer Information Sciences students learning programming; nursing students using course-specific software; English students writing papers using a word processor; noncredit students learning to use genealogy software; and students using campus computers to access off-campus data bases. By design, student labs are “open” although at some colleges a student computer ID card is required for access to campus computer labs in an effort to prevent, or limit, unauthorized access. However, some colleges are so committed to serving the community that people are rarely refused access to a computer, unless it is obvious that they are not students of the college and that they are interfering with the learning process. This very openness, while a strength of the institution, also provides an opportunity for possible unethical conduct.

A sample case study of a breach of ethical conduct

In the spring semester of 1994 a student gained control of the college's UNIX system. He was registered for the UNIX class taught by the CIS department. A problem first became evident when the other students in the UNIX class encountered problems accessing the system. Once users had accessed the system, they encountered additional problems, particularly with the printer. When students tried to access files in a subdirectory created by the instructor, they could not find the files. When the instructor tried to logon the system, he found that access had been denied. Data files created for the class were inaccessible, so students logged off the system and tried to logon again. Access was denied to the students. Shortly thereafter the system was totally inaccessible. Computer Services notified the appropriate academic Chair that a student had brought down the UNIX system and that Computer Services did not have the resources to restore the system. Specifically, Computer Services stated that the master password had been stolen, directory protection had been changed so that no one could use the editor, and all access to the system was denied. At this point in time the UNIX system was inoperative and a crisis was evident.

Solution to the sample case

After receiving information from Computer Services that a student had breached security, the academic Chair contacted the UNIX instructor. The instructor agreed to contact the student in question to ascertain exactly what commands the student had used to take control of the system and how to reverse those commands. After initially denying any involvement, the student did admit to planting a trojan horse on the system as part of an experiment for a paper he was writing about computer security. The commands the student used came directly from a textbook and the student claimed not to know the possible damage that the code could cause when he entered it. The student gave the instructor the new passwords and the instructor promptly accessed the system and issued new passwords. Extensive system work was required by several individuals before the system was totally repaired. In fact, all existing accounts on the system had to be purged, a backup created, and 116 new accounts created.

During this time the student was not given access to the system. A meeting of the principal parties involved was set up with the Dean of Students. The student met with the Dean of Students who advised the student of his rights, responsibilities and the consequences of his unethical behavior. The student was made aware of the possible courses of action available to the college ranging from admonition to expulsion. Based on the factors of this particular situation, the student was given a letter of reprimand and warned that a second violation would result in stronger disciplinary action. The student was given access to the system in order to complete course requirements.

Proposed solution to prevent future cases of this nature

The proposed solution to prevent future ethical violations of the computer system has several components. First, there must be an increased awareness by students of their rights and responsibilities with respect to computers. This can begin with rigorous enforcement of the College I.D. card policy. All students are given a copy of the Student Handbook which clearly states in boldface “Entrance to all computer labs require current I.D. cards”. The policy also clearly states that only currently enrolled students are permitted to use the computer labs. Enforcing this policy will allow lab assistants to more closely monitor student activity. For example, there are holders for the student I.D. cards on top of all monitors in the computer labs. If students are routinely taught to place their I.D. card on top of their monitor, lab assistants will easily be able to identify currently enrolled students. More importantly, it will reinforce to the students that security measures are in place and that ethical conduct on their part is expected.