Journal of Information Systems Education
FALL/WINTER 1998

Computing-Use Violations in Academic Settings

Heidi Perreault
Professor
Department of Computer Information Systems
Southwest Missouri State University
901 S National Ave
Springfield MO 65804
417-836-6319
heidiperreault@mail.smsu.edu

Nancy Keith
Professor
Department of Marketing and Quantitative Analysis
Southwest Missouri State University
901 S National Ave
Springfield MO 65804

Cases of computer abuse (Deloughry, 1994, Countering Mischief) at academic institutions are on the rise. Although most college administrators view computer abuse as a problem, they differ in their approaches to dealing with individuals who are guilty of computer-use violations. Some administrators submit all allegations of computer-use violations to campus security. Penalties for those found guilty of abuse range from a loss of computer privileges to criminal charges being filed. Other administrators support education and awareness campaigns. The assumption is that computer abuse can be curbed by making students aware of what is and what is not responsible use (Smith, 1992 and Malone, 1993.)

The purpose of this study was to determine the types of computer violations experienced by academic institutions and if students, faculty, staff, or individuals from outside the institution perpetrated the violations. Additionally, information on the types of actions taken by the institution against the perpetrator and opinions as to how individuals should be made aware of computer-related ethical and legal issues were sought.

LITERATURE OVERVIEW

Common computer-use violations at academic settings include unauthorized access to files, the sending of harassing or threaten messages, and the impersonating of another by manipulating electronic mail messages (Deloughry, 1994.) To protect information resources, most academic institutions assign passwords to authenticate authorized users. Only students, faculty, and staff who have explicit permission to read or change the data are allowed access to the files. Tuomy (1996) warned that passwords are not adequate because "they are subject to human fallibility" (p. 33). Users have been known to post passwords next to their computer, use their name or birth date as the password, and to incorporate passwords into startup procedures.

Sheehy and Trites (1995) acknowledged that passwords are inadequate. Another preventive measure is to build multiple security levels and to become stringent about identifying remote users. Passwords should allow a user access to specific areas of the computer network; they should not allow users to "roam freely" (Tuomy, 1996.) To prevent the misuse of passwords, users should be educated about the need for security. Data security needs to be "everyone's business" according to Romney (1995.)

At many academic institutions, computer-use violations are more of a nuisance than a threat to data security. Deloughry (1994) reasoned that the increase in the number of computer-use violations was attributed to both an increase in the number of computer users and the anonymity afforded the violator. Law-abiding citizens seem to feel "less accountable" for their actions when using a computer. An administrator at MIT believes it is often a case of students wanting to "prove their technical expertise" (Deloughry.)

When an incident of computer-related abuse is detected, the situation and the intent of the violator should be examined. The user may be unaware of the legal implications and may not recognize the violation as an ethical issue. Malone (1993) suggested that computer-use problems could be avoided by providing students opportunities to discuss moral and ethical issues associated with computer use. Students should be given a copy of the institution's computer-use policy, and the policy and penalties associated with misuse should be discussed in detail. Administrators in general agree with the use of stated policies and that a serious violation should be reported to authorities. They disagree on the amount of emphasis to put on less serious violations such as send-

ing annoying messages. The sentiment of many educators and administrators is that efforts should be directed toward educating users not toward policing them. Nonacademic computer services administrators share this attitude. Backhouse and Dhillon (1995) reported that large organizations worldwide are seeking "to increase understanding of and sensitivity to" responsible computer use. Administrators agree that there is a greater need to have a "higher level of awareness" among the workforce than to increase levels of security and enforcement.

In some cases, an individual responsible for a violation is punished. For example, a University of Illinois student was arrested after sending a life-threatening message to President Clinton. A similar fate awaited a Massachusetts Institute of Technology (MIT) student who operated a bulletin board to exchange copyrighted software. Many other cases, however, are never investigated. Administrators point out that they are not trained in investigative work nor do they have time to investigate all incidents of reported abuse. The number of violations in a month can be in the hundreds (Deloughry, 1994, Countering Mischief.)

Two generally accepted means for combating computer abuse at academic institutions is to have stated computer use policies and to educate users on acceptable behavior. Providing users with a copy of the institution's computer-use policy communicates computer use rules and associated penalties for inappropriate use. Parker (1993) found, however, that many academic institutions had no stated policy. He stressed that for policies to be useful they must be stated, communicated, and followed. Paone (1996) emphasized the need to evaluate services, update policies in relation to services offered, and to enforce all stated policies. Another tool for combating computer abuse is to make users aware of which actions are considered improper or unethical. Students and staff need to be educated as to what constitutes a violation. Some campuses have developed rules of computer etiquette that include a list of "do nots" such as not threatening people, destroying hardware, or copying software. A slightly different approach used by some institutions is to encourage students to think for themselves about what is responsible and ethical behavior when using the computer and computer networks. Rather than telling users what not to do, they provide guidelines for making ethical decisions. The responsibility to make judgments regarding what is appropriate behavior is shifted to the user.

RESEARCH OBJECTIVES AND PROCEDURES

A survey instrument was sent to directors of academic computing at colleges and universities. The directors' names and addresses were obtained from CAUSE. CAUSE is an organization for professionals responsible for computing resource management and support in higher education. Institutions ranging in size from under 500 to over 5,000 computer users and representing all geographic regions in the United States were included in the study. The directors were asked to provide information regarding incidents of computer abuse at their institutions for the most recent twelve-month period.

The information requested included the types of computer-use violations, who committed the violations, and the types of actions taken in response to violations. For those institutions that reported computer violations, information was requested regarding the existence and content of their computer-use policies to detect if computer-use violations were addressed in the document. The academic computing professionals also were asked to share their perceptions as to how individuals should be made aware of what constitutes a violation.

The goal of the study was to generate a listing of common types of computer-related security and/or ethical violations occurring in academic settings and to determine if the violations are addressed in computer-use policies. The specific research questions addressed by the study include the following.

(1) What computer-related violations have been reported within the past year?
(2) Who committed the violations?
(3) What types of actions/penalties were taken/assessed because of the violations?
(4) Are common violations included in a computer-use policy statement?
(5) How should computer users be educated as to what constitutes a violation?

FINDINGS

Academic computing directors provided input as to the types of computer violations their institution had recorded within the last academic year, who was responsible for violations, and the types of penalties associated with computer-use violations. The respondents also provided input on the content of their institutions' computing-use policies and gave their opinions as to how users should learn about computer-related ethical and legal issues. Responses reflect computer-use violations reported by182 academic institutions.

TYPES OF VIOLATIONS REPORTED

Sixty-two (62%) percent or 114 of the respondents indicated at least one reported computer-use violation during the past academic year. A listing of the types of violations reported and the percentage of institutions indicating at least one occurrence of each violation type is presented in Table 1. Some institutions do not have a formal process of reporting and/or recording incidents of computer violations; therefore, more institutions may have experienced incidents of computer-use violations than were reported.

Table 1: Type of violation and percentage of those institutions that reported incidents of computer violations that had at least one occurrence of the violation type.

Type of Violation	Percentage of Institutions Reporting Violation Type
Sending Obscene/Abusive Messages	68%
Violationg Copyright Laws	49%
Playing Computer Games	49%
Releasing Passwords	39%
Using Computer for Personal Financial Gain	18%
Cheating on Test or Assignments	12%
Other	11%

Note: Frequency based on 114 institutions reporting computer-use violations.

Sending obscene or abusive messages, violating copyright laws, playing unauthorized games, and releasing passwords were the types of violations listed most often as having been reported during the last year. Violations recorded by fewer than 20% of those institutions that reported computer-use violations were using the computer for personal gain, cheating on tests or assignments, and other. The types of abuses listed as "Other" included destroying files, spreading viruses, tampering with equipment, and impersonating another e-mail user.

Although the violation listed by the most institutions was "sending obscene/abusive messages," the most frequent type of violation is unknown because multiple occurrences of the same type of violation may have occurred at an institution. The listing of computer-use violations should be used to reflect the type of abuse occurring and not as a listing of the most typical (or common) violation.

The types of violations reported differ slightly from those reported by nonacademic institutions. The inappropriate use of email is a concern shared by businesses (Rapoport, 1997,) but unauthorized access was the violation reported by more organizations than any other violation during 1996 (Perreault & Keith, 1996.) The findings to concur with the report by Deloughry (1994) on academic computer abuses. Students continue to abuse email privileges.

PERPETRATORS AND PENALTIES

Students were identified most often as being responsible for the violations. Of the 114 institutions indicating computer violations, 75 reported students as the perpetrators. Individuals from outside the institution (not student, faculty, or staff) were listed by 25 institutions. Faculty and staff were listed by 16 and 10 institutions respectively as perpetrators. Nineteen institutions indicated the individuals responsible for violations were unknown.

Actions taken by institutions against a perpetrator vary. The types of actions taken are listed in Table 2. Most of the respondents indicated that violations are handled in-house. Suspending computer privileges or holding a conference to discuss the violation are the action taken by over half of the institutions that reported violations. Twelve respondents indicated that their institution had brought legal charges against an individual. The specific violation associated with the bringing of legal charges is not known.

Table 2: Type of action taken as a result of a computer violation and the number of institutions taking the action at least once in a 12-month period.

Type of Action Taken in Response to an Incident of Computer Abuse/Violation	Number of Instituions Reporting Having Taken Action
Computer Privileges	67
Conference held to Discuss Violation	66
Entry Made on Permanent record	16
Prosecution	12
Do Not Know Action Taken	8
Other (dismissal, suspension, restricted access, campous hearing)	18

Many administrators are reluctant to bring charges against students, faculty, and staff. The lack of punishment was a concern noted by many respondents. They felt the administration did not treat computer violations seriously and consequently neither did the students, faculty, nor staff.

POLICIES AND EDUCATION

Almost one third (32%) of the institutions reporting incidents of computer abuse did not have a stated computer-use policy. Those institutions with policies typically had a policy addressing common violations. At least 71% had a policy on ethical issues (including sending abusive messages), 64% had a policy on copyright resource use, 77% had a policy on authorized use (including playing games), and 67% had a policy dealing with authorized access and/or password security. As the literature indicated, having a policy does not prevent violations.

Both the academic computing professionals who indicated that their institution had experienced incidents of computer abuse and those that listed no reported incidents of computer abuse believe computer-use policies are an effective means for educating users on computing-related ethical and legal issues. All but 7 of the respondents indicated they favored using computer-use policies as a means of educating users about ethical and legal issues relating to computers. This is interesting because 67 of the 182 respondents indicated their institution did not have a computer-use policy. No reason for the lack of policy was given. A few comments were included regarding the lack of time or administrative support available to develop policies.

The second most popular means of educating users indicated by the respondents was including information on ethical use in computer classes. (A complete listing of the suggested methods for educating users as provided by the respondents is displayed in Table 3.) Eighty-two percent of the respondents selected "computer classes" as an appropriate means for users to learn about ethical and legal issues associated with computer use. This finding is supported in the literature (Malone, 1993; Smith, 1992.)

Table 3: Methods by which users should learn about ethical issues and legal concerns regarding computer use.

Methods for learning about ethical and legal issues relating to computer use	Numebr of respondents selecting methods
Computer-use policies	175
Computer classes	149
Self education	89
Other	23

The respondents had several suggestions for educating users other than using computer-use policies, computer classes, and self-education. Nine stated that in-service/workshops should be held for faculty, staff, and administrators. Others listed providing more information to users on ethical issues and what constitutes abuse. They suggested several ways for sharing that type of infor-

mation such as through newsletters, posters, computer system messages, user guides, electronic mail messages, university handbooks, and contracts requiring a student signature.

CONCLUSIONS AND DISCUSSION

Academic institutions are experiencing incidents of computer violations. Sending obscene or abusive messages, violating copyright laws, and playing computer games are the types of violations being reported. Some institutions indicated they expect that incidents of abuse are occurring but their institution has no formal mechanism for reporting or for recording incidents of abuse.

Perpetrators of the abuse included students, individuals from outside the institution, and faculty or staff. More institutions listed students as perpetrators than any other group. The disciplinary actions taken in response to a violation were suspending computer privileges and holding a conference to discuss the incident. Other actions listed by at least 12 institutions included making an entry on the perpetrator's permanent record and prosecution.

Some of the academic computing directors indicated they believed more severe penalties should be imposed upon individuals guilty of computer abuse. Others indicated that it is more important to educate users than to punish them. The comments reflect the two philosophies related to computer access. One philosophy is that it is a student's right to have access to technology, while the other view is that access to technology as a privilege granted to a student. The adopted philosophy will influence the types of actions taken in regard to violations. An institution viewing computer access as a privilege will be more likely to revoke access when a violation occurs. If access to technology is a student's "right," denying access will be a last resort (Deloughry, 1994.) Both philosophies on computer access endorse the publishing of computer-use policies.

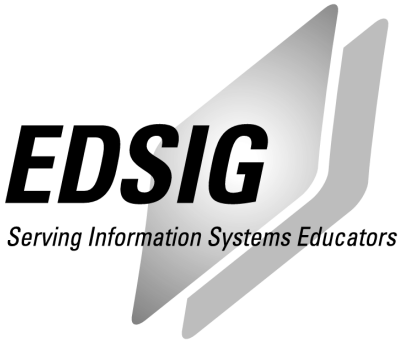
Approximately two thirds of the institutions participating in the study did have a computer-use policy and most of the policies contained information relating to common violations. The respondents felt that policy statements were important. Accrediting institutions also recognize the need for computer-use policies. As a requirement for accreditation, the Southern Association of Colleges and Schools requires microcomputer policies be "clearly stated and consistent with the institutional purpose and goal" (12). To be effective, the policies must clearly communicate to users their rights and obligations as an authorized user. Examples of what constitutes abuse should be included in the document. Policies alone, however, will not deter computer abuse.

The respondents agree that computer-related legal and ethical issues need to be part of a student's educational program. Over eighty percent of the respondents indicated users should be provided information on computer ethics and legal issues through both computer-use policies and through classes. The respondents noted that computer ethics should not be limited to a topic covered in computer classes. They stressed the need for computer-related ethics to be part of a total education program. As one respondent stated, "ethics are not restricted to the computer lab."

REFERENCE ENDNOTES

1. Deloughry, T. (1994, May 25). Countering Mischief. The Chronicle of Higher Education, A19-A20.
2. Smith, M. (1992). Professional Ethics in the Information Systems Classroom: Getting Started! Journal of Information Systems Education, (4), pp. 6-9.
3. Malone, D. (1993). The Ethical Issues of Automated Information Processing. Journal of Computer Information Systems, (33)3, pp. 82-84.
4. Tuomy, J. (1996, March). Data security: protecting the network. Managing Office Technology, pp. 33-34.
5. Sheehy, D. & Trites, G. (1995, September). Access denied. CA Magazine, pp. 50-52.
6. Romney, M. (1995, May). Computer Fraud—what can be done about it? The CPA Journal, pp. 30-33.
7. Backhouse, J. and Dhillon, G. (1995). Corporate Computer Crime Management: A Research Perspective. Computers & Security, (14)7, pp. 645-651.
8. Parker, R. (1993). A Study of Microcomputer Resource Policies at Two- and Four-Year Colleges and Universities. Journal of Information Systems Education, (5), pp. 27-30.
9. Paone, J. (1996, September 2). Firewall Fights Intranet threat. LAN Times. pp. 1, 22.
10. Rapoport, M. (1997, February 24). E-mailed racist, sexist messages no laughing matter. The Times-Union, Jacksonville Fl, p3.
11. Perreault, H. & Keith, N. (1996) Security Measures and Computer Fraud Issues in Industry, Refereed Proceedings of the Decision Sciences Institute Annual Meeting, Volume 2, p. 802.
12. Southern Association of Colleges and Schools. (1992-1993). Criteria For Accreditation. Atlanta, p. 49.

Information Systems & Computing
Academic Professionals



STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN 1055-3096