# Discovering and Disciplining Computer Abuse in Organizations: A Field Study[1]

By: Detmar W. Straub, Jr.
William D. Nance

Curtis L. Carlson School of Management
Information and Decision Sciences Department
University of Minnesota
271 19th Avenue South
Minneapolis, Minnesota 55455

## Abstract

*As information system (IS) managers and computer security administrators attempt to address what may be a serious and persistent problem of computer abuse in organizations, two important aspects must be considered: discovery of abuse incidents and discipline of perpetrators. This field study examines how IS managers address these two activities.*

*Data for the study were gathered using victimization surveys of 1,063 randomly selected members of the DPMA (Data Processing Management Association). Results of the study suggest that purposeful detection of abuse incidents is used less than other methods of discovering abuse. Furthermore, the results show that certain perpetrators are able to hide their identities and abusive activities. Based on these results, the study conclusions present a model that shows how security efforts should be managed in terms of security effort allocations and disciplinary actions.*

Keywords: Computer abuse, computer crime, security, management of computing

ACM Categories: K.4, K.4.2, K.6.4, K.6.m, K.7.m

## Introduction

This study addresses the ways managers of information systems and computer security uncover computer abuse and discipline computer abusers. It assesses risks being incurred, measures taken to detect abuse, and actions used to discipline abusers. The study was designed to identify current organizational and managerial responses to the computer abuse problem and to determine how managers can control damage from abuse.

### *The risk of being abused*

There is some evidence that organizations are often victimized by serious incidents of computer abuse (AICPA, 1984; Colton, et al., 1982; Hoffer and Straub, 1989; Straub, 1986a). Two previous studies (ABA, 1984; Research Institute of America, 1983) suggest that computer abuses cause annual losses in the millions, or even billions, of dollars in the United States alone. A recent study by Ernst and Whinney (Ernst & Whinney, 1989; LaPlante, 1987) reveals that 50–90 percent of U.S. firms suffer dollar losses annually from computer abuse.

There is also some evidence that computer abuse is likely to continue in the future. American society's growing computer literacy has created increasingly sophisticated users of technology. An undesirable side effect of this increased sophistication is that users are becoming more adept at commiting various types of computer abuse (Lee, et al., 1986; Makley, 1987; Spafford, 1989). Thus, even though organizations continue to develop and implement more protective security measures (Chaum, 1985; Clyde, 1987; Maude and Maude, 1984), computer abuse may continue to be a problem as we proceed into the 1990s.

---

[1] A substantially abbreviated version of this paper appeared in the European practitioner journal, *Information Age*, in July, 1988.

Funding for the study was provided by IRMIS (Institute for Research on Management Information Systems) at the Indiana University School of Business, the IBM Corporation, the Ball Corporation Foundation, and the MIS Research Center at the Curtis L. Carlson School of Management, University of Minnesota.

## *Management responses to abuse risks*

The vulnerability of modern computerized systems has led to the development of specialized computer security units in organizations and to the implementation of various countermeasures (Straub and Hoffer, 1988; Wood, 1987). Between 50 and 60 percent of organizations assign personnel to the administration of computer security on a full or part-time basis (Straub, 1986b). Most of these administrators are situated in the information systems (IS) area and have titles such as "director of data security," "manager of computer security," or "computer security administrator" (Straub, 1986a).

Many contingencies govern an organization's specific response to an act of computer abuse. The damage inflicted may affect the extent of the response as may the "hardness" of the case against the perpetrator (Goldstein, 1984). However, evidence now supports the view that vigorous enforcement of system access policies by active security administrators can lower future abuse (Straub, 1986b). It is important, therefore, for managers to understand the implications of their actions so they can respond accordingly.

### Deterrent and Preventive Actions

Security administrators employ a range of techniques to guard against purposeful or accidental system misuse (Perry, 1987a). Two classes of countermeasures—deterrents and preventives—have been found to be effective (Straub, 1986b). Deterrents are passive, administrative controls that take no active role in restricting the use of system resources. Examples include computer security awareness training sessions and distributed policy statements that specify conditions for proper use of the system. Preventives, on the other hand, screen access to the system to admit authorized users only. Preventives include physical restraints such as locks on computer equipment room doors and programmed restraints such as software locks on accounts, files, transactions, and data items.

### Detective Actions

Security administrators can also protect systems through vigorous detection strategies (Parker, 1983; Straub, 1986a). Detection is a proactive strategy that involves purposeful investigation of system activity to identify and follow up on possible irregularities (Parker, 1981). An abusive incident is "discovered" when the irregularity is verified. Detection strategies range from recording and tracking unusual activities to randomly scanning files to exception reporting (Parker, 1983; Straub, 1986a). Properly designed internal accounting and systems controls can enhance detection. Security administrators are assisted in their detection efforts by internal and external auditors (Perry, 1987b) who are responsible for testing for errors and irregularities that result in material losses, but who are not responsible for guaranteeing system integrity (AICPA, 1988). However, because many organizations rely on triggers from internal controls or accidental discovery of abuse (AICPA, 1984; Kusserow, 1983; Straub, 1986b), it appears that targeted activities to detect abuses are not widely implemented.

### Disciplinary Actions

In cases where a perpetrator has been identified, security personnel and systems managers may choose from a variety of potential administrative and judicial responses. They may disregard the consequences of the act and merely warn the offenders. They may even promote offenders in an attempt to buy their silence (Parker, 1983). Organizations may choose to discipline abusers by imposing internal sanctions such as suspension, fine, reprimand, or dismissal. Finally, they may report offenses to outside groups such as the police or the FBI and engage in civil and/or criminal prosecution.

Although organizations have the option of reporting offenses to outside groups, a high percentage of abuses are apparently never reported to law enforcement authorities (Sherizen, 1985; Solarz, 1987). Straub (1986a) found that only 5-10 percent of all abuse discovered by and known to organizations is reported to police. Solarz (1987) found that less than 5 percent of all discovered computer crimes are prosecuted. Given the amount of recent media attention on computer abuse, this lack of external discipline is discouraging.

# Study Background

Criminologists believe that discovered incidents of white collar crime represent only a small subset

of all white collar crimes, and there is evidence that this applies to computer abuse as well. Studies have found that as many as one half of computer-related crimes are discovered by accident (AICPA, 1984; Kusserow, 1983; Straub, 1986a; 1986b). It is possible that accidental discovery reveals most, if not all, computer abuse incidents not discovered by normal controls or detective activities. Past research on white collar and computer crime suggests, though, that this is unlikely. A more likely interpretation, and a critical assumption in this study, is that incidents of computer abuse go undiscovered much of the time.[2]

## Definition of computer abuse

Based on distinctions proposed by Kling (1980), computer abuse is defined in this study as unauthorized, deliberate, and internally recognizable misuse of assets of the local organizational information system by individuals. Possible abuses include violations against:

- **hardware** (and other physical assets associated with computers such as theft or damage to terminals, CPUs, disk drives, and printers)
- **programs** (such as theft or modification of programs)
- **data** (such as embezzlement or modifiction of data)
- **computer service** (such as unauthorized use of service or purposeful interruption of service)

It should be noted that some incidents where motivations were not apparent were also reported. As a result, the data included numerous borderline incidents, many of which were reported to be motivated by ignorance of proper professional conduct, in which the actual motivation behind the abuse was uncertain.

[2] Speculation beyond this, to sepcific estimates of undiscovered losses nationally, are probably unwarranted and misleading. The ABA report points out that even approximate numerical estimates are not possible, given the kind of data collected to date and the inexactness of that data (also Eagleson, 1986; Webster, 1985).

## Research questions

To address the most prominent computer abuse concerns of management and to suggest ways to deal with the threat, the study focused on two research questions:

*How is computer abuse discovered in organizations?*

*How are identified computer abusers disciplined?*

The next section discusses types of abuses, how they are discovered, and how abusers are disciplined. It also states several hypotheses that were tested in this study regarding these issues.

# Key Issues and Exploration Hypotheses[3]

What is currently known about the discovery of computer abuse and the discipline of abusers? Prior studies present frequency distributions of abuse by dollar loss category, offender motivation type, and victim industry type. They used victimization surveys (ABA, 1984; AICPA, 1984; Local Government Audit Inspectorate, 1981) and archival data gathered from media and police reports of abuse (Parker, 1976; 1981; Solarz, 1987). Unfortunately, these studies do not use statistical tests to answer questions about linkages between security administrators' activities and abuse, nor do they use rigorously validated research instruments. Nevertheless, these studies provide valuable insight into the abuse problem and background for the questions posed in this study.

## Discovery of abuse

This section addresses the first research question: How is computer abuse discovered in organizations? It is already known that many abuses are discovered by accident and many others by internal system controls, but that fewer are uncovered via independent, purposeful detection activities on the part of security officers

[3] All hypotheses are stated in null form. Hypotheses that utilize a one-sided test are accompanied by an alternative hypothesis that states the directionality of the hypothesized relationship.

or auditors.[4] What has not been studied is whether method of discovery differs among types of abuse and among target assets. The possible types of abuse and target assets analyzed in this study are:

**Abuse Types**
Unauthorized access
Destruction of system resource
Unauthorized distribution of system resource
Unauthorized duplication of data or programs
Unauthorized modification of data or programs
Unauthorized personal use of system resource
Theft

**Target Assets**
Computer service for personal use
Computer service available to other users
Data
Hardware
Programs

It would be helpful to know if specific discovery methods are more or less effective in uncovering certain abuse types or target assets. Finding, for example, that purposeful detection is closely associated with discovery of certain abuses while other abuses tend to be discovered through normal system controls enables security administrators to emphasize discovery techniques that are most effective in uncovering abuses of particular concern in their organization. Thus, linking method of discovery with these variables can help in allocating resources in the security and audit functions. H1 and H2 test the relationships between method of discovery, types of abuse, and target asset.

**H1: The method of discovery of computer abuse incidents is unrelated to abuse type.**

**H2: The method of discovery of computer abuse incidents is unrelated to target asset.**

Identification of offenders is another important objective in attempting to discover computer abuse. According to prior studies, perpetrators cannot be percisely identified up to 40 percent of the time (ABA, 1984). It would be useful to determine the circumstances under which offenders are most likely to be identified. Warfel (1986), for example, suggests that it is difficult to identify perpetrators of data manipulation abuses. Like method of discovery, knowledge in this area can suggest how security efforts can be redirected onto high payoff activities. Relationships between identification of computer abusers, type of abuse, and target asset are tested in H3 and H4.

**H3: Identification of offenders is unrelated to abuse type.**

**H4: Identification of offenders is unrelated to target asset.**

## *Disciplining abusers*

This section addresses the second research question: How are identified computer abusers disciplined? An organizational perspective provides insight into the tendency of organizations to respond to computer abuse incidents in certain ways. An individual perspective provides insight into managers' responses to computer abuse incidents. Both of these perspectives are addressed in the hypotheses on disciplining abusers.

From an organizational perspective, we examined two factors that may influence the disciplinary actions taken. The first, size, may be important because disciplinary actions may be related to the dollar value of assets to be protected. Larger organizations and larger EDP shops may be more likely than their smaller counterparts to have established policies and guidelines for handling violations. H5 and H6 test whether these policies include imposing stiff penalties for serious offenses. The second, industry, may be important because of the nature of the assets to be protected. Specifically, banking institutions are required by law to report certain kinds of computer-related frauds and embezzlements,[5] and they can be expected to take sterner measures against offenders (H7).

**H5: The overall size of the organization is unrelated to the severity of discipline imposed.**

[4] Prior works verify that accidental discovery of a problem occurs in about one third (AICPA, 1984; Straub and Hoffer 1988) to one half of all cases (Kusserow, 1983). Normal systems controls (such as internal controls) comprise 25–45% of all discovery methods (Kusserow, 1983; Straub and Hoffer, 1988), with only 9-25% of abuses discovered via purposeful investigation by security officers or auditors (Straub and Hoffer, 1988; AICPA, 1984).

[5] 12 Code of Federal Regulations 21.11.

**H5a: Larger organizations discipline computer abusers more severely than smaller organizations.**

**H6: The size of the organization's EDP department is unrelated to the severity of discipline imposed.**

**H6a: Organizations with larger EDP departments discipline abusers more severely than organizations with smaller EDP departments.**

**H7: The victimized organization's industry is unrelated to the severity of discipline imposed.**

**H7a: The financial industry disciplines abusers more severely than other industries.**

From an individual perspective, managers can take several steps to discipline computer abusers. One critical issue is self-regulation. Do people responsible for computer security (e.g., managers, security officers, auditors, and other high-ranking and high-privilegd users) receive relatively lighter punishments than lower-privileged users, or are punishments meted out equally? It has been suggested that senior executives are less likely to be detected and/or punished than lower-level employees (Data Processing Auditing Report, 1986). This hypothesis is tested in H8.

In most situations, it is likely that managers would make the punishment fit the crime and impose more severe punishments for more serious offenses. This is tested in two forms, a subjective comparison (H9) and a dollar loss comparison (H10). Another common perception is that abuses that are more strongly motivated will result in heavier penalties. The maliciousness of a saboteur or the greed of an embezzler, for example, should provoke a stronger managerial response than misguided playfulness or possible ignorance of proper system conduct. This proposition is tested in H11.

**H8: The offender's organizational position is unrelated to the severity of discipline imposed.**

**H8a. Computer abusers in lower-privileged organizational positions are disciplined more severely than abusers in higher-privileged positions.**

**H9: The perceived seriousness of the computer abuse is unrelated to the severity of discipline imposed.**

**H9a: Perpetrators of abuses that are perceived to be more serious are disciplined more severely than perpetrators of less serious abuses.**

**H10: The size of the dollar losses resulting from the computer abuse is unrelated to the severity of discipline imposed.**

**H10a: Perpetrators of abuses that result in larger dollar losses are disciplined more severely than perpetrators of smaller dollar loss abuses.**

**H11: The strength of a computer abuser's motivation is unrelated to the severity of discipline imposed.**

**H11a: Perpetrators of abuse who have stronger motivations for the abuse are disciplined more severely than perpetrators with weaker motivations.**

# Methodology

The study used a victimization questionnaire developed from criminological theory, previous victimization surveys, prior computer abuse instruments, and the computer abuse literature. The instrument was validated in three stages. Thirty seven systems professionals participated in extensive field interviews. Then 88 provided interviews and preliminary questionnaire responses. Finally, 170 responded to the pilot questionnaire. This validated questionnaire was mailed out to 5,489 randomly selected DPMA (Data Processing Management Association) members. The sample base that resulted was 1,063 respondents with reports on 268 separate abuse incidents.[6] The questionnaire and details of the validation process are found in Straub (1989).

A key question in this study was item 43, which reads "Please briefly describe the incident and what finally happened to the perpetrators." Responses to this free format item, which were

[6] To enrich the database, pilot survey data were combined with final survey data in cases where responses were clearly not duplicates. This procedure and other quality control procedures increased the incident sample and at the same time reduced the respondent sample.

reasonably complete across respondents, were coded according to the type of abuse, perpetrator identification, and disposition of the case, including displinary action.

## Data Analysis[7]

An initial set of tests for non-response bias was performed to ensure that respondents did not differ systematically from non-respondents. Two kinds of tests were used. First, "geographic comparisons" compared characteristics of the group that was mailed the survey with the group that responded. No differences were found, suggesting that information from non-respondents did not differ substantially from that of respondents based on geographic considerations. Second, timed "waves" of respondents were compared for variations on the primary independent and dependent variables. This test is based on the assumption that later waves adequately represent characteristics of non-respondents; since no differences were found, it was inferred that no systematic differences existed between early and late respondents. In summary, since respondents did not differ on either geographic or timing factors, it was concluded that the sample is not systematically biased and that the study findings are generalizable to the entire 36,000 person DPMA membership.

### *Analysis of discovery hypotheses*

One objective of this research project was to assess how organizations are able to successfully uncover incidents of computer abuse. Another objective was to determine how successful these organizations have been in identifying perpetrators of computer abuse.

Incidents of computer abuse were discovered by three methods: accidental discovery, normal system controls, and purposeful investigations (aka "detection"). As shown in Figure 1, 41 percent of the incidents were discovered accidentally (by either users or systems personnel); 50 percent were discovered by normal system controls; and only 16 percent were discovered by purposeful investigations.

[7] Summarized data tables and details of statistical tests used to analyze the research hypotheses are shown in the Appendix.

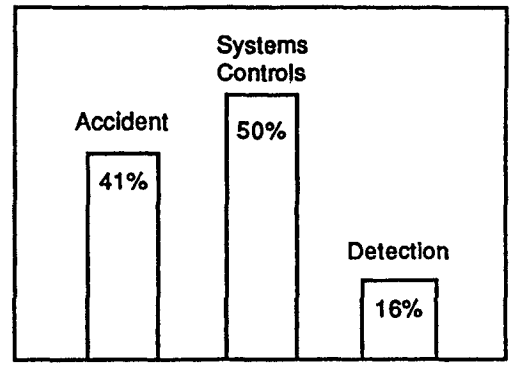


**Figure 1. Distribution of Discovery Modes (%)[8]**

Turning to the results of H1 and H2, there is little evidence to suggest that method of discovery is related either to type of abuse or to target asset. Only four significant relationships were found in 36 tests evaluating the two hypotheses. Since this was only slightly higher than the number of significant results that are expected by chance at a 5 percent level of significance, few, if any, conclusions can be drawn regarding relationships between method of discovery, type of abuse and target asset (H1 and H2: DO NOT REJECT).

Perpetrators of abuse were identified in 76 percent of the reported incidents. Regarding H3, four of seven tests revealed significant relationships between type of abuse and perpetrator identification (H3: REJECT, Table 1A). Duplication and personal-use abusers could be identified at a statistically significant level. Perpetrators of destruction and theft tended to remain unidentified. Regarding H4, four of five tests revealed significant relationships between target asset and perpetrator identification (H4: REJECT, Table 2A). People who abused data and computer service for personal use could be identified at a statistically significant level. Abusers of hardware and computer service to others tended to remain unidentified.

Several interesting conclusions arise from these findings. First, purposeful detection showed no

[8] Percentages exceed 100% because some incidents could only be uncovered through a combination of methods. For example, several cases arose where an irregularity was noticed accidentally, but the actual abuse incident was not "discovered" until follow-up detection activities were completed.

tendency to be either more or less effective in uncovering incidents of specific abuse types or target assets. This suggests that detective activities may not have targeted specific potential abuses and may have been "fishing expeditions" more than anything else. It also suggests that detection may be equally successful on all types of abuse and for all target assets.

Second, of the assets targeted for abuse, hardware and computer service disruption abuses were the least likely to result in the identification of the perpetrator. This points out one of the major prescriptive suggestions of the study:

**There is a need for increased organizational detection activities that focus on hardware and service disruption abuses because the perpetrators of such abuses have frequently been able to remain unidentified.**

## *Analysis of disciplinary hypotheses*

Another focal point of this study was the disposition of computer abuse incidents. Disciplines reported for incidents of abuse fell into one of three categories: "no discipline," "internal discipline," and "external discipline." Figure 2 indicates the breakdown, in percentages, for these discipline categories.

In increasing order of severity, internal disciplinary actions included reprimands, suspensions, fines, and terminations. The breakdown of internal disciplinary actions, in percentages, is

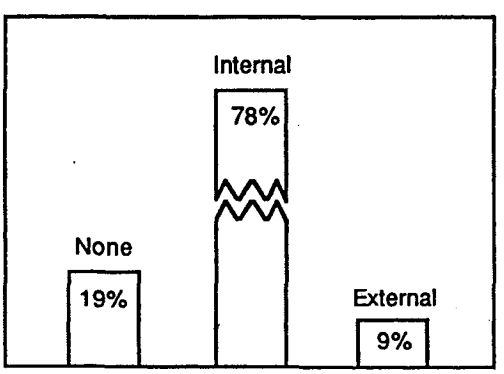


**Figure 2. Categories of Discipline (%)[9]**

[9] Percentages exceed 100% because of the possibility of both internal and external disciplines for any single incident.

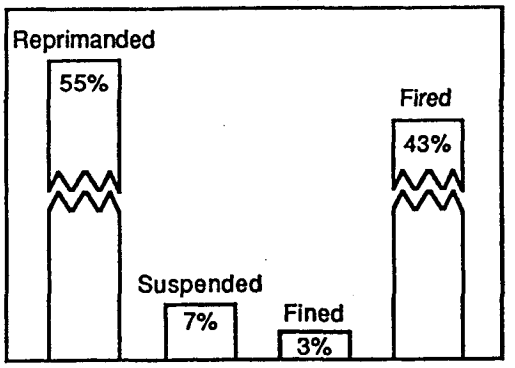


**Figure 3. Internal Discipline (%)**

shown in Figure 3. External disciplines, again in increasing order of severity, included police reports, prosecution, indictment, and conviction. The number of actual incidents in these external disciplinary categories (for incidents in which the perpetrator was identified) is shown in Figure 4.

Of the 268 discovered computer abuse incidents, 24 (9 percent as shown in Figure 2) were reported to external authorities. However, perpetrators in 12 of the 24 externally reported incidents were not identified and could not be prosecuted. Of the other 12 incidents where the perpetrator was identified, ten were prosecuted for an overall prosecution rate of 4 percent (10 of 268 incidents). In incidents where the perpetrator was known, the rate was still only 5 percent (10 of 211 incidents). Overall, 3 percent (seven of 268 incidents) of all discovered incidents resulted in convictions. This is in line with prior reports that have found that a very low percentage of discovered computer abuse incidents results in convictions (Leinfuss, 1986; August, 1983). However, since prior research has shown that threat of sanctioning is a deterrent to abuse (Straub, 1986b), the 70 percent (seven of 10) conviction rate of prosecuted cases clearly suggests that computer abuse may be reduced by prosecuting abusers more frequently and more severely.

In testing the discipline severity hypotheses, several interesting findings arose. No relationship was found between overall organizational size and severity of discipline (H5: DO NOT REJECT, Table 3A). EDP department size, however, was found to be related to discipline severity (H6: REJECT, Table 4A). Organizations with larger EDP

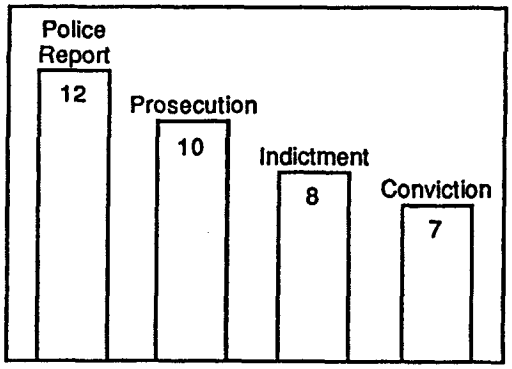


**Figure 4. External Discipline (# Incidents)**

departments tended to discipline abusers more severely than organizations with smaller EDP departments. The differences between these two findings suggest that organizations with larger dollar investments in EDP facilities may appreciate the need for strong computer abuse policies but that organization-wide policies for treating abuse have not yet been established in many organizations.

One interesting finding of the study is that hypothesized differences in discipline severity between industries, particularly between financial institutions and all other industries, were not present (H7: DO NOT REJECT, Table 5A). Because financial institutions are required by law to report material computer abuse losses, it was anticipated that financial institutions would report and prosecute abusers more frequently than other industries. This was not supported; no industrial groups tended to discipline abusers more or less severely than other industrial groups.

In looking at the severity of discipline within the financial services industry, however, an interesting related finding turned up. Several instances of abuse resulted in large dollar losses that were not reported to the police. Financial institutions reported 24 abuse incidents, 12 of which resulted in dollar losses. Of the 12 reported losses, only four were reported to the police. The range of losses on the reported incidents was $15,000-$150,000 while the range of losses on the unreported incidents was $400-$10,000. Of the eight unreported incidents, seven resulted in losses of $500 or more; four resulted in losses of $1,000 or more; and two resulted in losses of $5,000 or more. The perpetrator was identifed in all four incidents resulting in losses of $1,000 or more. Since federal laws state that banks must report losses of $1,000 or more in cases where a suspect is identified,[10] it appears that some organizations may have violated federal laws by failing to report material computer-related losses.

At the individual level, a highly significant and interesting finding was the association between offender position and discipline severity (H8: REJECT, Table 6A). It was found that high-privileged users are discipline less severely than medium-privileged or low-privileged employees. Table 1 highlights this favored treatment of high-privileged personnel (Table 6A provides a complete list of organizational positions classified by level of privilege). This favored treatment is not only a distortion of justice, it is also unwise because it diminishes the deterrent impact on other employees.

**Table 1. Discipline by Position**

| Level of Privilege | Not Disciplined | Disciplined |
|---|---|---|
| High | 11 | 20 |
| Medium | 3 | 42 |
| Low | 3 | 36 |

Regarding the relationship between seriousness of the abuse and the severity of the resulting discipline, the study generated incongruous results. Inspection of the data (Tables 7A and 8A) suggests that both measures of abuse seriousness were positively associated with severity of discipline, but a statistical association only existed between perceived seriousness of abuse and discipline severity (H9: REJECT, Table 7A). Seriousness of abuse in dollar terms was unrelated to discipline severity (H10: DO NOT REJECT, Table 8A).

There is a ready explanation for this discrepancy. In many instances actual dollar loss may have been minimal while the potential for loss was significant (Straub, 1986a). An alternative explanation is possible respondent bias. The incidents reported are based on respondent recall,

[10] 12 Code of Federal Regulations 21.11.

and respondents may have based their perceptions of seriousness on the severity of the discipline imposed. If true, then the implied causality between seriousness and severity may be backwards.

Finally, strength of perpetrator motivation was found to be related to the severity of the discipline imposed (H11: REJECT, Table 9A). Although the statistical tests reveal differences in discipline severity across the four groups of perpetrator motivations, they do not show which motivations are likely to be disciplined at significantly higher or lower levels of severity. Examination of the group means, however, shows that abuses motivated by ignorance of proper conduct had the lowest average discipline severity, whereas perpetrators motivated by misguided playfulness had the highest average discipline severity.

## Discussion

A normative model of the detection and discipline process is presented in Figure 5. Computer abuse is initially observed either by internal controls, by accident, or by purposeful detective activity. If internal controls or accident trigger the observation, detective activity to verify the occurrence of the abuse and to identify the perpetrator follows. Once the abusive incident has been verified, it can be said that the computer abuse has been discovered. Further assessment of the damage and circumstances of the abuse then allows for smoother recovery and appropriate disciplinary measures. Making the punishment fit the crime includes reporting certain activities to enforcement agencies.

This model formulates an approach to security administration. As this administrative activity is gradually incorporated into organizations' technology management practices, it will undergo numerous, inevitable changes. This evolution needs to be carefully managed so that system abuse can be brought into line with other organizational control objectives.

Based on the evidence in this study and other empirical work, the administration of computer security can be improved in several specific ways. First, security administrators should give increased attention to detection in their repertoire (cf. Bequai, 1985). Detection may work equally well in discovering computer abuse incidents of all types and targets. Furthermore, a high level of visible detective activity also has the desirable effect of deterring future abusers (Straub, 1986b). Second, organizations should report serious abuse incidents to authorities more frequently.

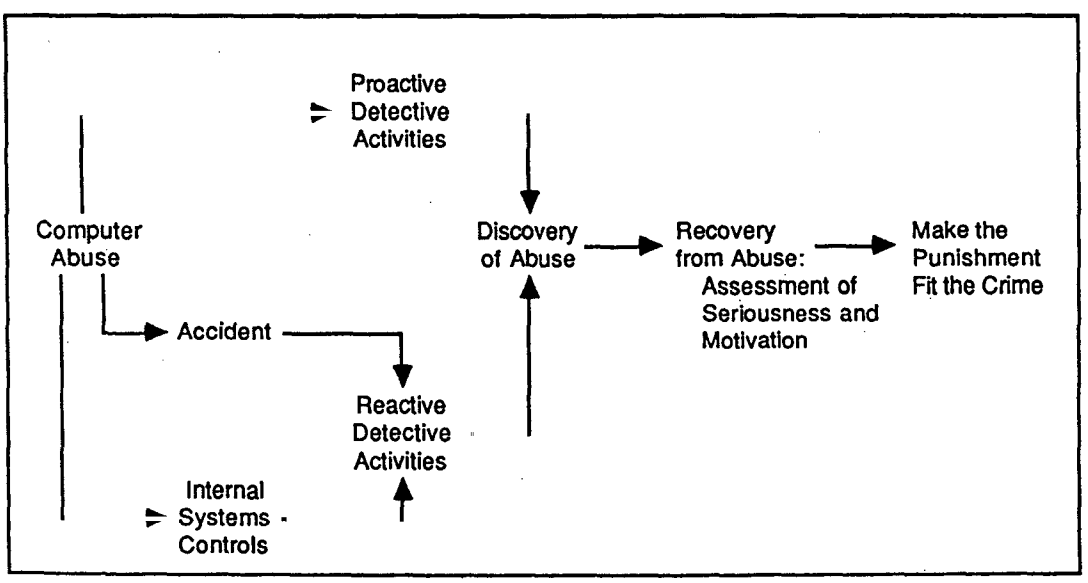


**Figure 5. Model for Detection and Discipline of Computer Abuse**

Although financial institutions may be in legal jeopardy for not fully prosecuting people who commit computer fraud and abuses, they are by no means alone in this low level of reporting. Third, perpetrators holding entrusted positions in the organization should not be given highly preferential treatment. Such treatment is undesirable for three reasons: (1) it has negative impact on effective deterrence, (2) it poses moral and ethical questions, and (3) it may also expose the organization to subsequent legal liabilities. Finally, organizations should discipline abusers motivated by personal gain or malice at least as harshly as they discipline abusers who are simply "playing around." If they fail to do so, their policies may not be successful in deterring the most dangerously motivated abusers.

While many of these heuristics are simply good general management practices, computer systems expose the organization to particular vulnerabilities and need to be dealt with explicitly. In this context, it has been pointed out that a million dollars is as easy to steal as one dollar when the computer is used (Parker, 1976; 1981). There is a place for leniency in violations of organizational codes of conduct. With computer abuse incidents, however, serious violations should be punished to the full extent of prescribed internal sanctions and the law because of the potent deterrent effect of such practices.

## References


ABA. "Report on Computer Crime," pamphlet prepared by the Task Force on Computer Crime, American Bar Association, Section on Criminal Justice, 1800 M Street, Washington, D.C. 20036, 1984.

AICPA. "Report on the Study of EDP-Related Fraud in the Banking and Insurance Industries," pamphlet from the American Institute of Certified Public Accountants, 1211 Avenue of the Americas, New York, NY, 1984.

AICPA. "The Auditor's Responsibility to Detect and Report Errors and Irregularities," Statement on Auditing Standards #53, American Institute of Certified Public Accountants, 1988.

August, R.S. "Turning the Computer into a Criminal," *Barrister*, Fall 1983, p. 13ff.

Bequai, A. "A Security Checklist," *Computerworld*, December 23, 1985, p. 33.

Chaum, D. "Security without Identification: Transaction Systems to Make Big Brother Obsolete," *Communications of the ACM* (28:10), October 1985, pp. 1030–1044.

Clyde, A.R. "Insider Threat on Automated Information Systems," 4th Insider Threat Identification System Conference, Bethesda, MA, August 1987.

Colton, K.W., Tien, J.M., Tvedt, S., Dunn. B. and Barnett, A.I. "Electronic Fund Transfer Systems and Crime," U.S. Department of Justice, Bureau of Justice Statistics, Washington, D.C., 1982.

*Data Processing Auditing Report.* "Who Is a Computer-Fraud-Prone Employee?" July 1986, pp. 6–7.

Eagleson, D. "Of Sticky Wickets, Tricky Digits," *Systems User*, July 1986, p. 6ff.

Ernst & Whinney. "The 1989 Computer Abuse Survey: A Report," pamphlet, Ernst & Young, 2000 National City Center, Cleveland, OH 44114, 1989.

Goldstein, B. "Investigating Computer Crime," *Computer Crime Digest*, February 1984, pp. 8–10.

Hoffer, J.A. and Straub, D.W. "The 9 to 5 Underground: Are You Policing Computer Crimes?" *Sloan Management Review*, Summer 1989, pp. 35–43.

Kling, R. "Computer Abuse and Computer Crime as Organizational Activities," *Computer Law Journal* (2:2), 1980, pp. 186–196.

Kusserow, R.P. "Computer-Related Fraud and Abuse in Government Agencies," unpublished paper, U.S. Dept. of Health and Human Services, Washington, D.C., 1983.

LaPlante, A. "Computer Fraud Threat Increasing, Study Says," *Infoworld* (18), May 1987, p. 47.

Lee, J.A., Segal, G. and Steier, R. "Positive Alternatives: A Report on the ACM Panel on Hacking," *Communications of the ACM* (29:4), April 1986, pp. 297–299.

Leinfuss, E. "Computer Crime: How Deep Does It Go," *MIS Week*, February 10, 1986, p. 41.

Local Government Audit Inspectorate. "Computer Fraud Survey," unpublished paper, sponsored by the Department of the Environment, Great Britain, 1981.

Makley, W.K. "Computer Security's Worst Enemy: Management Apathy," *The Office* (105:3), March 1987, pp. 115–116.

Maude, T. and Maude, D. "Hardware Protection Against Software Piracy," *Communications of the ACM* (27:9), September 1984, pp. 950–959.

Parker, D.B., *Crime by Computer,* Scribner's, New York, NY, 1976.
Parker, D.B. *Computer Security Management,* Reston, Reston, VA, 1981.
Parker, D.B. *Fighting Computer Crime,* Scribner's, New York, NY, 1983.
Perry, W.E. "Security Problems are People Problems," *Government Computer News,* March 27, 1987a, pp. 27–28.
Perry, W.E. "An Introductin to EDP Auditing," *Auerbach Data Security Management,* 82-03-30, July–August 1987b.
Research Institute of America. "Safeguarding Your Business against Theft and Vandalism," *Computer Crime Digest,* November 1983, p. 5.
Sherizen, S. "Shortcomings of Computer Crime Law," *Computerworld,* November 25, 1985, p. 17.
Solarz, A. "Computer-Related Embezzlement," *Computers & Security* (6:1); February 1987, pp. 49–53.
Spafford, E. "Crisis and Aftermath," *Communications of the ACM* (32:6), June 1989, pp. 678–687.
Straub, D.W. "Computer Abuse and Computer Security: Update on an Empirical Study," *Security, Audit, and Control Review* (4:2), ACM Special Interest Group journal, Spring 1986a, pp. 21–31.
Straub, D.W. *Deterring Computer Abuse: the Effectiveness of Deterrent Countermeasures in the Computer Security Environment,* unpublished dissertation, Indiana University School of Business, Bloomington, IN, 1986b.
Straub, D.W. "Validating Instruments in MIS Research," *MIS Quarterly* (13:2), June 1989, pp. 147–167.
Straub, D.W. and Hoffer, J.A. "Computer Abuse and Computer Security Administration: A Study of Contemporary Information Security Methods," IRMIS Working Paper #W801, Indiana University School of Business, Bloomington, IN, 1988.
Warfel, G.H. "Identification Technology," *Auerbach Data Security Management,* 84-01-10, July–August 1986.
Webster, W.H. "Technology Transfer, Industrial Espionage and Computer Crime: The Problems We Are Facing," *Computer Crime Digest,* January 1985, pp. 1–5.
Wood, C.C. "Information Systems Security: Management Success Factors," *Computers & Security* (4:6), August 1987, pp. 314–320.

## About the Authors

**Detmar W. Straub** is assistant professor of management information systems at the University of Minnesota where he teaches courses in systems and pursues research at the Curtis L. Carlson School of Management. Detmar has published a number of studies in the computer security management arena, but his research interests extend as well into emerging information technologies and theory and measurement of key IS concepts. Besides prior publication in the *MIS Quarterly,* he has also been published in *Communications of the ACM, Sloan Management Review, Journal of MIS,* and *Computers & Security.* His professional associations and responsibilities include: associate director, MIS Research Center, University of Minnesota; associate publisher of the *MIS Quarterly;* editorial board memberships; and consulting with the defense and transportation industries.

**William D. Nance** is a doctoral candidate in management information systems at the University of Minnesota's Curtis L. Carlson School of Management. He has published articles in *SIM Network, Information Age,* and *Michigan Investor.* He has also presented papers at several international conferences, including the International Conference on Information Systems, and is coauthor of a casebook titled *Using Software in Auditing.* His research interests include use of information technology in auditing and other control environments, ethical issues in organizations and information systems, management of the computer security function, and impacts of decision support systems as knowledge work support tools.

# Appendix

## Table 1A. H(3): Identification of Perpetrators × Type of Abuse Actual (Expected)[11]

| Type of Abuse | Other Type Perpetrator Not Identified | Other Type Perpetrator Identified | Abuse Type Perpetrator Not Identified | Abuse Type Perpetrator Identified | Pearson Chi-Square | p-value | Yates Correct p-value |
|---|---|---|---|---|---|---|---|
| Access | 33 (29) | 108 (112) | 19 (23) | 94 (90) | 1.673 | .196 | .256 |
| Destruction | 40 (45) | 179 (174) | 12 (7) | 23 (28) | 4.757 | .029* | .051 |
| Disclosure | 49 (46) | 177 (180) | 3 (6) | 25 (22) | 1.840 | .175 | .268 |
| Duplication | 52 (48) | 184 (188) | 0 (4) | 18 (14) | 4.987 | .026* | .054 |
| Modification | 48 (44) | 165 (169) | 4 (8) | 37 (33) | 3.449 | .063 | .100 |
| Personal Use | 52 (45) | 166 (173) | 0 (7) | 36 (29) | 10.798 | .001* | .002 |
| Theft | 33 (43) | 179 (169) | 19 (9) | 23 (33) | 18.957 | .000* | .000 |

INTERPRETATION:

1. Perpetrators of **Destruction** and **Theft** abuses tend to remain unidentified.
2. Perpetrators of **Duplication** and **Personal Use** abuses tend to be identified more frequently than other abusers.

* $p \leq .05$

[11] Several tables summarize Chi-square tables used in the data analysis. In order to obtain sufficient cell sizes in each table, the data was collapsed into a series of 2x2 Chi-square tables where each dimension of a given table was categorized as binary based on the existence of the variable of interest. Each row represents one 2x2 Chi-square table.

To explain the coding method more clearly the following discussion explains the meaning of values included in the Access row of this table. The first number in a category (i.e., not in parentheses) is the actual number of cases in the category; the second number (in parentheses) is the expected number based on marginal probabilities.

| | Other Type Perpetrator Not Identified | Other Type Perpetrator Identified | Abuse Type Perpetrator Not Identified | Abuse Type Perpetrator Identified | Pearson Chi-Square | p-value | Yates Correct p-value |
|---|---|---|---|---|---|---|---|
| Access | 33 (29) | 108 (112) | 19 (23) | 94 (90) | 1.673 | .196 | .256 |

- **Other Type Perpetrator Not Identified** is the number of abuse incidents that were not Access where the perpetrator was not discovered.
- **Other Type Perpetrator Identified** is the number of abuse incidents that were not Access where the perpetrator was discovered.
- **Abuse Type Perpetrator Not Identified** is the number of Access abuse incidents where the perpetrator was not discovered.
- **Abuse Type Perpetrator Identified** is the number of Access abuse incidents where the perpetrator was discovered.

**Table 2A. H(4): Identification of Perpetrators × Target Asset Actual (Expected)**

| Target Asset | Other Asset Perpetrator Not Identified | Other Asset Perpetrator Identified | Target Asset Perpetrator Not Identified | Target Asset Perpetrator Identified | Pearson Chi-Square | p-value | Yates Correct p-value |
|---|---|---|---|---|---|---|---|
| Service for Personal Use | 38 (31) | 96 (103) | 22 (29) | 107 (100) | 4.769 | .029* | .042 |
| Disruption of Service | 46 (51) | 177 (172) | 14 (9) | 26 (31) | 3.979 | .046* | .073 |
| Data | 47 (39) | 123 (131) | 13 (21) | 80 (72) | 6.378 | .012* | .018 |
| Hardware | 41 (52) | 188 (177) | 19 (8) | 15 (26) | 24.249 | .000* | .000 |
| Programs | 45 (46) | 157 (156) | 15 (14) | 46 (47) | .142 | .706 | .839 |

INTERPRETATION:

1. Abusers of **Hardware** and **Service Disruptions** tend to remain unidentified.
2. Abusers of **Computer Service for Personal Use** and **Data** tend to be identified more frequently than other abusers.

* $p \leq .05$

**Table 3A. H(5): Severity of Discipline × Total Organizational Assets**

| | < 5M | 5–100M | 100M–1B | > 1B |
|---|---|---|---|---|
| Number of Incidents | 32 | 34 | 27 | 28 |
| Average Severest Discipline[12] | 3.03 | 2.76 | 3.74 | 3.89 |

Kruskal-Wallis[13] = 9.78; df = 8; p = .281.

INTERPRETATION:

1. There is no significant difference in severity of discipline based on organizational size as measured by total assets.

[12] The severity ranking is as follows:

1. No Discipline
2. Reprimanded
3. Suspended
4. Fined
5. Fired
6. Reported to Police
7. Prosecuted
8. Indicted
9. Convicted

[13] The Kruskal-Wallis test uses individual data values, but the data presented in these tables are summarized. The statistical tests cannot be replicated using the summarized data.

**Table 4A. H(6): Severity of Discipline × EDP Budget**

| | < 1M | 1–8M | > 8M |
|---|---|---|---|
| Number of Incidents | 53 | 46 | 26 |
| Average Severest Discipline | 2.45 | 3.70 | 4.04 |

Kruskal-Wallis = 18.07; df = 7; p = .012*

INTERPRETATION:

1. Organizations with larger EDP budgets discipline abusers more severely than organizations with smaller EDP budgets.

*$p \leq .05$.

**Table 5A. H(7): Severity of Discipline × Industry**
**Actual (Expected)**

| Industry[14] | Other Industry, No Discipline | Other Industry, Some Discipline | This Industry, No Discipline | This Industry, Some Discipline | Pearson Chi-Square | p-value | Yates Correct p-value |
|---|---|---|---|---|---|---|---|
| Manufacturing | 16 (18) | 89 (87) | 5 (3) | 11 (13) | 2.482 | .115 | .222 |
| Government | 18 (18) | 87 (87) | 3 (3) | 13 (13) | .025 | .874 | 1.000 |
| Education | 17 (19) | 91 (89) | 4 (2) | 9 (11) | 1.827 | .176 | .335 |
| Computer Service Bureaus | 19 (18) | 87 (88) | 2 (3) | 13 (12) | .193 | .660 | .940 |
| Finance | 19 (17) | 78 (80) | 2 (4) | 22 (20) | 1.699 | .192 | .316 |
| Utilities | 18 (18) | 87 (87) | 3 (3) | 13 (13) | .025 | .874 | 1.000 |

INTERPRETATION:

1. No industry disciplines computer abusers more or less severely than other industries.

[14] Industries included in the research questionnaire but not shown in this table were excluded because they contained an insufficient number of organizations to be able to perform a useable Chi-square analysis.

**Table 6A. H(8): Severity of Discipline × Organizational Position**
**Actual (Expected)**

| Level of Privilege | Not Disciplined | Disciplined | Total |
|---|---|---|---|
| High | 11 (5) | 20 (26) | 31 |
| Medium | 3 (7) | 42 (38) | 45 |
| Low | 3 (5) | 33 (31) | 36 |
| Total | 17 | 95 | 112 |

Pearson Chi-square = 13.770; p = .001*

INTERPRETATION:
1. Computer abusers in highly privileged organizational positions are not disciplined as often as abusers in medium or lower-privileged positions.

**Organizational Positions Included in Each Level of Privilege**

| High-Privilege Positions | Medium-Privilege Positions | Low-Privilege Positions |
|---|---|---|
| Top Executive | Data Entry Staff | Accountant |
| Security Officer | Application Programmer | Clerical Personnel |
| Auditor | System Analyst | Student |
| Controller | EDP Machine Operator | Consultant |
| Manager/Supervisor | Other EDP Staff | |
| System Programmer | | |

* $p \leq .05$.

**Table 7A. H(9): Severity of Discipline × Perceived Seriousness of Abuse**

| | Of Negligible Importance | Of Minimal Importance | Serious | Extremely Serious |
|---|---|---|---|---|
| Number of Incidents | 6 | 43 | 58 | 26 |
| Average Severest Discipline | 2.00 | 2.84 | 3.26 | 4.62 |

Kruskal-Wallis = 9.44; df = 3; p = .024*

INTERPRETATION:
1. Incidents perceived by the respondent to be more serious were disciplined more severely than incidents perceived to be less serious.

* $p \leq .05$.

**Table 8A. H(10): Severity of Discipline x Dollar Losses**

| | < 1000 | 1000–10,000 | 10,000–50,000 | > 50,000 |
|---|---|---|---|---|
| Number of Incidents | 14 | 18 | 11 | 6 |
| Average Severest Discipline | 2.21 | 3.17 | 5.73 | 7.67 |

Kruskal-Wallis = 34.95; df = 29; p = .206

INTERPRETATION:

1. Incidents resulting in larger dollar losses were not disciplined more severely than incidents resulting in smaller dollar losses at a statistically significant level.

**Table 9A. H(11): Severity of Discipline x Perpetrator Motivation**

| | Ignorance of Proper Conduct | Misguided Playfulness | Personal Gain | Maliciousness |
|---|---|---|---|---|
| Number of Incidents | 27 | 40 | 31 | 18 |
| Average Severest Discipline | 2.74 | 4.42 | 2.87 | 3.06 |

Kruskal-Wallis = 9.83; df = 3; p = .020*

INTERPRETATION:

1. There are significant differences in the severity of discipline imposed on perpetrators based on the motivation behind the abuse.

* $p \leq .05$.