Protecting Organizational Information Resources

MICHAEL D. WYBO
DETMAR W. STRAUB, JR.
University of Minnesota

This paper presents an overview of the empirical evidence concerning the nature of computer abuse against organizations and viable control mechanisms. A model of perpetrator motivation is presented and General Deterrence Theory is proposed as an appropriate theoretical basis for the design and implementation of computer abuse countermeasures. In this theoretical context, specific actions that computer security specialists, information systems managers, and EDP auditors can take to reduce the likelihood of computer abuse in their organizations are proposed.

The use of computer-based technologies in the processing and storage of organizational information resources is standard practice in the 1980s. Many of today’s business procedures and services are possible only because of the computer’s ability to process large numbers of individual transactions quickly and accurately. However, as with any other technological extension of man, computer systems are subject to abuse, and their failure to perform in the manner intended can endanger the very enterprises they were designed to serve and protect. The computer in its roles as an information processor, deliverer, and repository has become a vehicle and/or target for abuse. The potential threat to organizations from intentional misuse of computer systems and organizational data is real. Furthermore, management and law enforcement have been slow in responding to fundamental changes being wrought by the computer, and this sluggish response may be adding to the uncertainty surrounding the computer abuse issue.

Defining Computer Abuse

The terms “computer fraud,” “computer crime,” and “computer abuse” are often used interchangeably to mean the intentional misuse of computer system assets such as hardware,
data, programs, and computer service (Parker, 1976, 1981; Straub, 1986b).

Fraud denotes deception, the “intentional perversion of truth in order to induce another to part with something of value or to surrender a legal right” (Webster, 1967). This first definition describes what is thought of as computer crimes, that is acts that can involve criminal or civil sanctions. These acts range from a clerk’s addition of a small amount of overtime pay to his own paycheck every week to sophisticated embezzlement schemes involving large sums of money. A second definition of fraud—an “act of deceiving or misrepresenting” (Webster, 1967)—is more generic and intimates activities that simply violate organizational policies or mores; for example, an employee’s use of the organization’s computer system during off hours to run his own information service bureau.

Neither of the terms, computer fraud nor computer crime, connotes acts of sabotage. Sabotage may not necessarily involve deception and may not necessarily be illegal. Organizations nevertheless may find it desirable to punish the offense in order to deter future violations. In order to reduce confusion and include as many possible facets of the phenomena under discussion, the term computer abuse is used to refer to all of the above mentioned types of misuse of information resources.

The term computer abuse as used here refers to the deliberate misuse of information resources. Although it is conceivable that system users may unintentionally perpetrate incidents of computer abuse, such unintentional incidents may be avoided through adequate informational and training programs. Intentional abuses have the potential for much more serious consequences and for being more difficult to detect and deter.

Lastly, the term computer abuse is used to refer to the misuse of organizational information resources by individuals. Computer abuse may be conceived in terms of (a) organizational or individual perpetrators. From a social and legal perspective, the Organization/Organization, Organization/Individual, and Individual/Individual perpetrator/victim combinations of abuse require social regulation outside the organizational environment. Responses to abuse by individuals against organizations, however, occur largely within the organization (Straub & Nance, 1989) and, in all likelihood, will continue to be handled internally in spite of newly enacted federal and state laws directed specifically at computer abuses. Internal handling predominates because abuses are embarrassing and perceived as a sign of lax security (Straub, 1986b). These Individual/Organization abuses therefore hold the greatest promise for improving management of the risk. The bulk of the research into computer abuse to date, moreover, has been in this domain.

The operational definition of computer abuse used in the remainder of this discussion is based on distinctions suggested by Kling (1980) and elaborated by Straub and Nance (1989):

Computer abuse is unauthorized, deliberate, and internally recognizable misuse of assets of the local organizational information system by individuals, including violations against:

1. hardware (and other physical assets associated with computers such as theft or damage to terminals, CPUs, disk drives, and printers)

2. programs (such as theft or modification of programs)

3. data (such as embezzlement or modification of data)

4. computer service (such as unauthorized use of service or purposeful interruption of service).
The Extent of Computer Abuse

To accurately know how much computer abuse is really occurring is difficult at best and may well be impossible. In the first place, even the best current evidence concerning the size of the abuse problem has polled only a subset of all the abuse that actually takes place. Reported abuse—that which has been reported to the police or media—and discovered abuse—that which has been discovered by an organization but not necessarily reported to the media or police—are very likely only a portion of all the abuse that occurs (Straub, 1986a, 1986b). Because discovered and reported abuse have necessarily provided the sampling frame for all of the empirical work that has been performed to date, we have no first-hand data on computer abuse in toto.

An estimate that occurs frequently in the literature is that unreported and undiscovered computer abuse may be as much as six times as high as known abuse (e.g., Bailey & Rothblatt, 1984). Such estimates are offered with the caveat that it is simply not known from first-hand data how extensive the problem really is. Case histories and sample survey data indicate that organizations report a wide range of losses (AICPA, 1984; Colton, 1982a, 1982b; Straub, 1986a; Whiteside, 1978). The American Bar Association survey (ABA, 1984) reported total dollar losses of approximately one half billion dollars for 72 firms out of a sample base of 148. The task force concluded from this evidence that computer abuse was an “enormous” problem in the U.S. (p. xii). Furthermore, “known and verifiable losses” in this study averaged in the millions of dollars. A large percentage of major firms are reportedly uncovering one or more serious incidents of abuse each year with, according to an Ernst and Whinney study, dollar losses being experienced by 50% to 90% of these victims (LaPlante, 1987). Moreover, large dollar losses do not appear to be a function of the sample from which the data is collected. It is very likely that losses of over $100,000 will occur periodically within a group of firms. One study (Straub, 1986b) of 211 victimized organizations reported five losses of more than $100,000 while a prior study of 35 organizations (Straub, 1986a) reported one loss of more than $2,000,000.

Methodological difficulties make accurate estimation of the true extent of computer abuse problematic (Taber, 1980; Skogan, 1981). Despite problems inherent in the investigation of computer abuse, empirical research by several authors has revealed some characteristics about computer systems and the act and perpetrators of computer abuse that hold significant potential for guiding successful organizational responses to the problem. In addition, this body of evidence supports the application of certain well accepted theoretical perspectives on how the computer abuse problem might be curbed while at the same time refuting the validity of other perspectives. The results of this body of empirical and theoretical literature are summarized in this paper and used to generate a set of recommendations for specific action by computer security specialists, EDP auditors, controllers, and information systems managers.

First, computer abuse is shown to be a unique organizational problem, distinct from other types of “manual” fraud and requiring special attention for its control. Next, a framework for thinking about the motivations of computer abusers and empirical evidence concerning abuser motivations is presented. The following section presents a review of alternative approaches to controlling computer abuse and argues that General Deterrence Theory is an ap-
Appropriate theoretical base for designing computer abuse controls. Last, based on the theoretical and empirical material in the previous sections, specific suggestions for controlling computer abuse in organizations are presented.

Computer Abuse as a Distinct Organizational Issue

Although it has been argued that computer abuse in many respects may not be inherently different from “manual” abuse (Kling, 1980), computer abuse does differ from the more traditional forms of fraud, embezzlement, or theft in that it exposes organizations to unique vulnerabilities that raise a unique set of control problems. This fact forces organizations to view and address it as a distinct organizational problem.

Several characteristics of computer technology and its use in organizations are important in understanding and controlling the computer abuse problem. Three important characteristics are the nature of computerized information systems, the growing importance of end user computing in large organizations, and the development and adoption of telecommunications technologies.

The Nature of Computer Information Systems

Several important characteristics distinguish computer information systems from their manual counterparts. These are:

High vulnerability. The high concentration of electronically stored information contributes to the efficiency of computerized information processing. It also contributes to the risk that sensitive data can be destroyed, altered, or stolen (Wilkinson, 1982). A file drawer full of sensitive information can be stored on a compact medium and carried out of the organization in a coat pocket. The contents of that same file drawer of documents could be destroyed with a simple magnet leaving no trace that they had been tampered with.

Violation of the principle of separation of duties. Conceptually, computer-based information processing violates the principle of separation of duties (at least two independent processes should control each phase of a transaction). But with computers, the various subsystems or functional areas of the organization process their information through a single processor and store it in a common working memory area or a common set of storage devices (Wilkinson, 1982). Checks and balances provided for by separate transactional controls may be invalidated in such a system.

System vulnerabilities are easily exploited. In a practical sense, the exploitation of a system vulnerability, once recognized, can be just as easily exploited a thousand times as once (Parker, 1976). This exploitation can be programmed to occur in the absence of any human agent, at a time when the system is operating normally, and in ways that covers tracks and makes detection or discovery extremely difficult.

Large amounts of data are easily manipulated. Schemes to defraud, which require massive manipulation of data not possible under manual systems, become achievable with computer based systems (Parker, 1976). In this respect computer technology makes new types of fraud possible.

Impersonal nature of systems. Computer abuse is never perceived directly by others while the act is being perpetrated. The perpetrator must never face any human guard of the organization’s assets. Because computer abuse is carried out against an impersonal machine, and what the perpetrator often perceives to be an impersonal organization, amateurs find it easy to rationalize their actions (Parker, 1980, 1983).
The Rise of End-User Computing

A second phenomenon with potentially serious implications for the incidence of computer abuse is the increase in many large organizations of end-user computing (EUC). EUC is the discretionary use and/or development of information systems by the principal beneficiaries of the system’s output. Users of an information system may program, enter data, operate, and have responsibility for entire information systems (Rockart & Flannery, 1983). EUC activities now account for a large part of all computing.

In their study of the EUC phenomenon, Rockart and Flannery (1983) found more than half of the end-user systems surveyed were servicing the information needs of entire departments. About one-fifth of the time, end-user systems carried across departments and functions. In some cases continuous access to end-user developed systems was essential for the functioning of one or more major departments. For these reasons, EUC has become an important component of the firm’s overall information management activities.

Clear risks in the operation and use of end-user applications will occur in the data integrity and data security arenas (Alavi & Weiss, 1985). While organizations have established some central EDP control over their large databases and systems, controls are virtually nonexistent in EUC. A study of 190 end users who developed and operated systems that used data from larger “production” systems found, for instance, that half of these end users had to rekey data into their own systems by hand (Rockart & Flannery, 1983). This situation greatly increases the likelihood of unintentional error and loss of data integrity as well as the opportunities for intentional abusive acts (Alavi & Weiss, 1985).

As a single group, application programmers abuse systems most frequently. However, the potential risk from EUC is highlighted by the fact that three categories of frequent end users (clerical personnel, functional area personnel, and managers) together account for the majority of computer abuses (Straub & Hoffer, 1988; Wong, 1985; Parker, 1981).

Some system users, such as systems programmers, EDP auditors, controllers, and security officers, can be considered to have “high privilege” access to the organization’s computing resources. As persons in positions of trust, high privilege users have carte blanche access to computer services, data, and programs. They have wide-ranging capabilities for accessing system files and programs, even those belonging to other users. The question of whether high-privileged users, such as systems programmers and security officers, cause more damage and greater losses in their abusive acts than those with less privilege is a legitimate one. Yet Straub (1986b) found that high privilege is not a factor in predicting computer abuse. Analyzing exposure by evaluating the number of high privilege users on the system, hence, appears to be an unwarranted risk evaluation technique. *

Some trusted employees, however, are clearly more dangerous to organizations than others. Managers tend to commit larger abuses but appear to be less severely punished upon apprehension (Straub, 1987a; Straub & Nance, 1989). Yet support is lacking for a commonly held belief that clerical staff are a high security

*This technique is known as Exposure Analysis. Exposure Analysis asserts that system losses are a function of exposure, which occurs when numerous high privileged users are granted access to a system (Parker, 1981). Greater numbers of high privileged users, therefore, should be associated with higher losses from abuse, a hypothesis simply tested if data on both variables has been collected.
risk, a relationship that has proved to be statistically insignificant (Straub, 1986b). Clericals do commit more abuses than their managers, but they are characteristically smaller, which reinforces a common sense interpretation of the situation.

Risks in the Development and Use of Telecommunication Technologies

Telecommunication technologies permit the transfer of large amounts of data among individual computers and information systems. These electronic linkages between computer systems also represent a gateway to an organization’s computing resources through which computer abuse may be perpetrated, potentially from anywhere in the world. Though the bulk of malicious abuses are perpetrated by insiders or employees of the organization, there are signs that individuals from outside the organization are developing new ways to subvert organizational systems through telecommunications. One example of the seriousness of the outside threat are the recent computer “virus” attacks against networks (Markoff, 1988).

Computer viruses are programs that are embedded or embed themselves in other legitimate programs or files. They can be introduced into a computer system through the physical transfer of files from one system to another or can propagate themselves through networks of connected computers. These rogue programs, once activated, can destroy data stored in the system or usurp control of computer resources such as the system’s memory or mass storage devices. Virus programs may reside in a host system until some predetermined event causes them to activate themselves and do their damage. Normal system backup procedures may only serve to archive existing virus programs along with legitimate programs and data (Dewdney, 1989).

In summary, the nature of the computer technologies underlying automated information systems, the way in which computerized information systems are being used in organizations, and the openness of computer systems to “infection” from the environment through telecommunications channels all serve to distinguish computerized information systems from their manual counterparts. In addition, these differences demonstrate that the problem of securing computerized information systems is distinct from that of securing manual systems and require that organizations conceive of and face computer abuse as a distinct organizational issue.

The Motivation of Computer Abusers

There are virtually an infinite number of ways to categorize motives of computer abusers. Criminologists like Zimring and Hawkins (1973) and Chambliss (1967) have argued that motivation has a bearing on how to control antisocial behaviors. Conceiving of the motivations for computer abuse through a framework that links motives to controls allows us to determine appropriate responses to particular motivational types. Such a framework has been developed by Straub and Widom (1984). The Motivation-Control typology classifies the motivations of computer abusers by strength of motivation. The four types of motivation described by their model are outlined below. Figure 1 links these motivational types to recommended control measures and examples of offenders for each type. Motivations of any given individual may vary from Type I to Type IV in different situations at different times (cf. also Parker, 1983).

Ethical ignorance is a motivation found in borderline abusers. These abusers may have some ethical conflict with respect to utilizing the computer system, though not a strong sense of wrong-doing. They are, nevertheless, violating the intentions of the asset owner. Acting within their professional capacities, these abusers lack knowledge that their use of the computer is not acceptable to the owner of the information asset.

Personal gain as a motivation occurs
when a perpetrator is aware that what he or she is doing is wrong or illegal but continues in spite of this knowledge. Inducements for professional or personal gain override the perpetrator’s normal fears of stigma and punishment.

Antisocial motivations occur when perpetrators are aware that their activity is socially unacceptable but proceed in spite of all sanctions. Perpetrators may actually be reinforced by the antisocial values of their subculture.

Corruption is a motivation when perpetrators have a clear sense of wrongdoing but believe they will escape the consequences of their actions by their mastery of the situation. Corrupt persons in high positions can dictate terms to lower ranking members of their organizations, thereby making prevention of corruption motivated abuse almost impossible.

Empirical Findings on Motivation

Straub (1986b) used a variation of the Motivation-Control Model in classifying data about motivation. Study data indicates that offenders were motivated first by desire for personal gain (30%), second by ignorance of proper professional conduct (26%), third by misguided playfulness (24%), and fourth by maliciousness (10%), as illustrated in Figure 2. It should be noted that, although the definition of computer abuse focuses on deliberate actions by perpetrators, respondents to this study reported incidents where the motivations of the perpetrator were not clear. Many of these ambiguous motivations were reported as ignorance of proper professional conduct, in effect conferring the benefit of the doubt on the motivations underlying the reported incident. The misguided playfulness category includes incidents such as sending or distributing humorous messages or playing computer games on the system, incidents indicative of ignorance of proper conduct but whose motivations respondents felt they could identify as a clear violation of organizational norms.

As the Motivation-Control Model suggests, it may be possible to deter abuses of the

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Control</th>
<th>Sample Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Ethical Ignorance</td>
<td>Deterrence by policy information</td>
<td>Borderline abusers</td>
</tr>
<tr>
<td>II</td>
<td>Personal Gain</td>
<td>Deterrence by detection and</td>
<td>Amateur criminals</td>
</tr>
<tr>
<td></td>
<td></td>
<td>punishment</td>
<td>White collar criminals</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Embezzlers</td>
</tr>
<tr>
<td>III</td>
<td>Anti-social Motives</td>
<td>Prevention by access control</td>
<td>Career Criminals</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>System hackers</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Deranged individuals</td>
</tr>
<tr>
<td>IV</td>
<td>Corruption</td>
<td>Detection by surveillance</td>
<td>Corrupt high officials</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Corrupt experts</td>
</tr>
</tbody>
</table>


Figure 1: Motivation-Control Model

Figure 2: Motivations of Computer Abusers
first three types, but not malicious abuse (Straub & Widom, 1984). Since maliciousness is an “expressive” motivation (as with so-called "crimes of passion"), potential abuses that result from it are likely to be much more resistant to the rational deterrents available to systems security administrators. It is fortunate, therefore, that maliciousness is a much less frequent motivator.

In many ways, computer abuse is a typical amateur, white-collar crime or antisocial behavior (Bequai, 1981; Parker, 1981; Sokolik, 1980). As such, it is perpetrated by persons who, in the pursuit of their occupations, normally abide by organizational policies and society’s laws (Sokolik, 1980). Sanctions, therefore, may be able to significantly reduce abuse. Either out of ignorance, a desire for pecuniary gain, or a wrong-headed playfulness, most abusers are willing to violate social norms, but are not so strongly motivated that either deterrent or preventive measures cannot inhibit them (Parker, 1981; Straub & Widom, 1984). The incidence of abuse as a result of misunderstanding between management and employees is undoubtedly very high (Straub & Hoffer, 1988).

**Approaches to Controlling Computer Abuse**

**Deterrent, Preventive, and Detective Controls**

The Motivation-Control Model proposes that there is a set of controls most appropriate for each abuser motivation. With computerization of the workplace over the last several decades, organizations have upgraded their control systems (Manuel, 1984; Walden, 1985), many of which have focused on deterrents (e.g., administrative policy statements), and on preventives, both software-based (e.g., user ID/passwords) and non-software-based (e.g., physical security of computer resources).

The computer security model in Figure 3 depicts the process of deterring, preventing, and detecting computer abuse incidents. The primary objective of computer security is, in fact, to minimize undiscovered abuse through a combination of deterrent, preventive, and detection activities. Many potential perpetrators are deterred by administrative policies, employee training, and visible security functions. Some abusers are not deterred, however, and their

---

**Figure 3: Computer Security Model**

---

attempted abuse must be thwarted by preventives. If the preventives work, the attempt is foiled. If the preventives fail, however, detection is the last avenue in attempting to uncover abuses.

This model and the motivational data from Figure 2 are revealing. Ignorance and misguided playfulness are examples of ethical ignorance, a motivation subject to control by deterrence through policy information. Stronger deterrents, therefore, may be able to curb over half of the abuses now occurring. Preventive measures, moreover, may be useful in those cases where personal gain is the motivation. In essence, approximately three quarters of identified incidences of computer abuse are predicted to be responsive to deterrent and preventive controls. What this evidence suggests about management practices should be of particular use to computer security administrators. Deterrents are clearly not a sufficient condition for inhibiting abusive behavior. However, in an evaluation of deterrence research to date, a blue ribbon panel commissioned by the National Research Council of the National Academy of Sciences concluded in 1978 that “the evidence ... favors a proposition supporting deterrence more than it favors one asserting that deterrence is absent” (Blumstein, Cohen & Nagin, 1978, p. 7). Since 1978, findings for a causal linkage have continued to receive support.*

Relevance of General Deterrence Theory to Computer Abuse

In all likelihood, computer abuse is a typical white-collar crime, a crime that, according to the theorists, may well be explained by General Deterrence Theory (Sokolik, 1980; Parker, 1981). Andenaes (1975) and others, for example, suggest that General Deterrence Theory is robust in explaining white-collar crimes...
because of the predominantly pre-planned, non-violent nature of crimes of this type. In white-collar crimes—crimes which violate occupational regulations (Geiss & Meier, 1979)—offenders most often make a rational choice in committing an abusive act (Buikhuisen, 1974). Especially strong evidence for the efficacy of deterrents in situations similar to computer abuse is found throughout the literature (Sokolik, 1980).

“Computer abuse, in sum, is in many cases an instrumental crime that can be deterred.”

Activities of the Computer Security Staff

What are the appropriate activities for those assigned the task of managing security? Before examining this issue in detail and suggesting how to prioritize resources, it is important to delineate the entire range of functions performed by computer security officers, as well as their present time allocations. Administrative roles in I/S security differ significantly from organization to organization, but their tasks can be generally classified into four areas:

1. Information (data) security
2. Physical security
3. Disaster recovery
4. User awareness training

In their information (data) security role, security officers focus on protecting data resources from deliberate misuse through electronic access paths. Effective measures of data security are designed to prevent, detect, and recover from intentional misuse of electronic assets as well as deter potential computer abusers. Both hard, active controls such as passwords and software restrictions, and soft, passive controls such as distributed policy statements, employee contract clauses, and violations reports are administrative controls employed by security officers. In this role, security officers use a variety of informational channels in conveying policies on the proper use of systems including publicized EDP policies, informal discussions, and organizational meetings. Approximately 51% of security officers’ time is presently spent performing this role (Straub & Hoffer, 1988).

The focus of physical security is on controlling physical access to system resources including processors, peripherals, and media. The security staff is charged with insuring that only authorized persons have physical access to these...
resources and that physical misuse of the system will not cripple the future functioning of the organization. In this role, the security administrator is responsible for seeing that unauthorized personnel do not have physical access to system resources from the mainframes in secured computer rooms to micros distributed throughout offices and production lines.

Disaster recovery involves the design and implementation of measures to insure the continuous operation of key information systems in the event of major damage to computing facilities. Such catastrophes are not necessarily the result of abusive activity, that is, they can also be purely accidental. In either case, the security officer must have a carefully articulated plan to allow the organization to recover data and programs and continue computerized operations. It has been shown that some 32% of security officers’ efforts are being directed toward disaster recovery and physical security (Straub & Hoffer, 1988).

User-awareness training focuses on raising employee awareness of their responsibilities regarding the organization’s information resources, on the consequences of abusing these resources, and on providing employees with the necessary skills to fulfill their responsibilities. Employees’ system authorizations, methods for changing passwords, methods for archiving PC-based systems and data, and other topics that have a bearing on protecting system assets from misuse are examples of the content of awareness training activities. This training is frequently included in employee orientation programs. Security officers spend about 11% of their time in this kind of training activity (Straub & Hoffer, 1988).

Deterring Computer Abuse Through Information

From the standpoint of controlling computer abuse, the roles of data security and user training are clearly key parts of the effort, and are especially important in deterring future computer abuse. In this effort, certain informational channels appear to be more useful than others for conveying organizational policies about proper system usage. Hoffer and Straub (1989) found that organizations used the channels as listed in Figure 4. As this table shows, informal administrative measures were used by many security officers, whereas security violations reports were utilized at a lower rate, specifically by those with security software in place. The organizations surveyed in this study tended to use, on average, four different informational channels.

How the message is conveyed to system users is clear enough, but what is the content of this message? First, system users must be told as precisely as possible what their data responsibilities are, and even more importantly, that they will be held accountable for safeguarding these information assets. The assignment of data responsibilities is itself a complicated process that occurs during the course of a vital records classification program or during system development.

As part of these activities, security officers assign access privileges to system resources on a need-to-know (Parker, 1981) or need-for-job basis. Clerical staff entering and maintaining data for order entry must have access to order data; they do not need, nor should they be given,
access to invoice payment data. Because of their job requirements, it may be necessary, however, to give them access to certain printers or terminals outside of their workstation. By the same token, managers, who are the one group of trusted employees statistically associated with higher dollar losses from abuse (Straub, 1987a), should not by default be given full access privileges to data under their jurisdiction. It may be sufficient in many cases for managers to be permitted to view certain data, without being permitted to change it. Changes should all be channeled through standard operating procedures involving clerical employees.

Second, system users must be told unequivocally that security violations will be sanctioned, in accordance with the seriousness of the offense, but without exception. Penalties ranging from reprimand and firing on the one hand to criminal and civil prosecution on the other should be specified. The effectiveness of such “disincentives”—an active security staff who help set data security policy and monitor the system environment and the specification of penalties for computer abuses—have been found to significantly lower computer abuse (Straub, 1987b).

**Security Software Used to Prevent and Detect Computer Abuse**

Security software is useful both in preventing and detecting computer abuses. Nance and Straub (1988) studied security software systems being administered by information systems security staffs and came to some interesting conclusions. This study attempted to gain insight into the kind and number of security software packages in use by a subset of organizations that employed some security staff. Of the groups with at least a nominal security staff in place, a surprising 27% reported not utilizing operating system security at all. This statistic is curious in that password access controls for user accounts is the default for virtually all major commercially available operating systems. What is possible is that respondents did not regard this fundamental level of security sufficient to answer the question in the affirmative.

Of this same sample, 32% had engaged one or more DBMS access control facilities and 18% were using security features built into their fourth generation languages. Given the power and versatility of these software features, one can argue that these percentages are too low for effective security.

Another questionnaire item asked for information about specialized security software, such as ACF-II (Access Control Facility II), IBM’s RACF (Resource Access Control Facility), Top Secret, Guardian, and the like. Respondents gave data on both purchased products, such as those above, and in-house developed software. According to returns from the security administrator group, 23% had one or more specialized software systems in active use. Of this group, 61% had only purchased products, 13% had only in-house products, and 26% had some of each. From the perspective of numbers of systems, respondents reported that vendor products were preferred to in-house products by a margin of better than 2 to 1.

Security software has been found to be instrumental in curbing computer abuse (Straub, 1986b), but the introduction of sophisticated packages must be carefully managed lest the implementation backfire and cause more harm than good. It has been recommended (Straub, 1986b) that specialized packages be initiated only in mature security environments; that suggestion is repeated here as a practice for consideration.

By way of summary, then, software access control facilities are being implemented to some degree or another in organizations having security administrators. Simpler tools, such as operating system security, are being used more extensively than sophisticated ones, such as the specialized packages, as might be expected. Readily available vendor software is preferred to in-house software.
Detection of Computer Abuse by Computer Security Officers

What role should detection play in the repertoire of security administration? Detection of computer abuse is an activity that falls primarily in the domain of information (data) security, with some detections falling in the physical security area. At present, most information security efforts appear to take the form of preventive activities, such as assignment of passwords and read-write-execute privileges, and deterrent activities. This, at least, was the case with one pre-test interview group reported by Straub (1986b). Few purposeful investigative activities seem to be in widespread practice. Apparently less than 15% of abuses are now being detected by security officers or auditors. Most abuses were discovered by accident (32%) or by normal systems controls (45%) rather than by either security officers (8%) or by internal (4%) or external auditors (0.5%) (Straub, 1986b).

Yet, by and large, it appears that abuse detected by investigative activities of security officers does not differ statistically from accidently discovered abuse (Straub & Nance, 1989). Different methods of discovery turn up the same types of abuse. This leads us to believe that the nature of undiscovered information systems abuse is likely very similar to that of system abuses that have been revealed thus far. Improved detection procedures, therefore, promise not only to discover more abuses as they are committed, but should also deter future abuse. In short, much more can be done, and needs to be done, in the way of detective activities on the part of computer security investigators (Clyde, 1987; Dunn, 1982).

Conclusions

This paper has addressed fundamental questions concerning the threat of computer abuse to the organization’s information resources. Computer abuse is a unique phenomenon and deserves study as such. Characteristics of computer information systems, and the extent to which organizations rely on them, expose organizations to unique vulnerabilities that raise a unique set of control problems.

Indications are that the problem of computer abuse is very possibly a serious one. There is a distinct possibility that we are seeing only the tip of the iceberg, in which case discovered abuse is only a small portion of all the computer abuse occurring. All organizations are at some risk and should make conscious efforts to control the problem.

The vast majority of computer abuse is accomplished by people within the organization. Empirical evidence shows that the majority of computer abuse is committed by computer users working in functional business departments (Straub, 1986b). It has also been argued that computer abuse is typically a white collar crime to which established theories and straightforward control measures can be applied. Restricting the access of privileged users has been found not to be an effective control measure, however.

The majority of computer abuse is thought to be responsive to controls available to computer security staffs. Strong deterrents and certain preventive measures can theoretically control a significant percentage of potential abuses. What is essential is that laws and policies be established to give organizations the tools to treat the problem as a serious one. First and foremost, organizations need to establish a professional security function to effectively deal with computer abuse.

References


Michael D. Wybo is a Ph.D. candidate in MIS at the Carlson School of Management, University of Minnesota. His research interests include the structure of the IS function, organizational information processing, the management of data as a corporate resource, and the characterization and measurement of organizational environments.

Detmar W. Straub, Jr., is an assistant professor of MIS and associate director of the MIS Research Center at the Carlson School of Management, University of Minnesota. His research interests include the management of information security, MIS theory and construct development, and emerging information technologies.
Related Content

The Selection of the IT Platform: Enterprise System Implementation in the NZ Health Board
Maha Shakir and Dennis Viehland (2005). *Journal of Cases on Information Technology* (pp. 22-33).
www.irma-international.org/article/selection-platform-enterprise-system-implementation/3137/

The FIFTH Perspective: Extending the Balanced Scorecard for Outsourcing
www.irma-international.org/article/fifth-perspective-extending-balanced-scorecard/3691/

eBay, Inc.: The Online Auction Industry
www.irma-international.org/article/ebay-inc-online-auction-industry/44569/

Goals and Requirements for Supporting Controlled Flexibility in Software Processes
www.irma-international.org/article/goals-requirements-supporting-controlled-flexibility/43718/

Managing Vendor Records for Monographic E-Collections at a Medium-Sized Academic Library
Aiping Chen-Gaffey (2014). *Teaching Cases Collection* (pp. 22-40).
www.irma-international.org/chapter/managing-vendor-records-monographic-collections/82638/