1988

AN INVESTIGATION INTO THE USE AND USEFULNESS OF SECURITY SO TWARE IN DETECTING COMPUTER ABUSE

William D. Nance
University of Minnesota

Detmar W. Straub
University of Minnesota

AN INVESTIGATION INTO THE USE AND USEFULNESS OF SECURITY SOFTWARE IN DETECTING COMPUTER ABUSE

William D. Nance
Detmar W. Straub
Curtis L. Carlson School of Management
University of Minnesota

ABSTRACT

Computer security remains an important issue in the management of organizational information systems. Losses resulting from computer abuse and errors are substantial, and IS managers continue to cite security and control as a key management issue. With continued expansion of distributed data processing and storage, the need to both prevent and detect violations also increases. This latter aspect, detection of computer abuse incidents, is the focus of this study.

This empirical study examines the prevalence and sophistication of security software system installations across the United States. Using a victimization survey of 528 randomly-selected DPMA members, the study examines discovered incidents of computer abuse in organizations and attempts to identify relationships between comprehensive (i.e., sophisticated) security software and successful discovery of abuse.

More comprehensive security software was found to be associated with greater ability to identify perpetrators of abuse and to discover more serious computer abuse incidents. Larger organizations used both a greater number and more sophisticated security software systems than smaller organizations. Wholesale/retail trade organizations used less comprehensive software than average, while manufacturing organizations and public utilities used more comprehensive software. Surprisingly, no relationships were found between the maturity of an organization's security function and the number and/or sophistication of security software systems utilized.

1. INTRODUCTION

Concerns over computer security continue to play an important role in the management of organizational information systems. Losses resulting from *intentional abuse* of computer systems appear to be substantial; in fact, they have been described as "enormous" by the American Bar Association (1984). The ABA survey reported total dollar losses from computer abuse of approximately $.5 billion per year in only 72 firms. Losses from *unintentional misuse* of systems, or error, further compound the problem (Alavi and Weiss 1985). Evidence for the importance of security is also provided by the frequency with which security and control is cited as a key management issue by I/S managers (Brancheau and Wetherbe 1987; Dickson, et al. 1984; Sprague and McNurlin 1986).

Because of heightened realization of the importance of I/S security to organizational survival, research has been growing on effective techniques for reducing abuse. The picture which is emerging supports the intuitive notion that internal controls and other forms of computer security can minimize computer abuse. Policy statements and an active security administration function, for example, are believed to reduce the number of abuse incidents (Straub 1986a). Deterrence is further provided through increased detection activities (AICPA 1984) and through appropriate punishment of perpetrators of abuse (Straub and Nance 1987). Cumulatively, these findings suggest that organizations with more proactive security functions significantly reduce their risk.

2. STUDY CONTEXT

As computerization of the workplace has progressed over the last several decades, organizations have upgraded their control systems (Manuel 1984; Walden 1985). Most of these control systems tend to focus 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).

However, deterrent and preventive countermeasures are not foolproof; abuse incidents occur and can only be discovered "ex-post facto." The problem is that organizations tend to rely on normal systems controls and accidental discovery to detect abuses which slip through the protective net. Straub and Nance (1987) report that only one of six of abuse incidents is discovered by proactive detection activities, possibly because detection activities tend to be "fishing expeditions" and are not targeted enough to be successful. The contention is that "security administrators should give increased attention to detection" (p. 27). Thus, a sound organizational computer security strategy not only requires utilization of deterrent and preventive countermeasures, but also requires a repertoire of detective activities to uncover incidents which slip through prior security nets.

The computer security model in Figure 1 depicts the process of preventing and detecting computer abuse incidents. The primary objective of computer security is to minimize undiscovered abuse through a combination of deterrents, preventives, and detection activities. Many potential perpetrators are deterred by administrative policies, employee training, and visible security functions. Some abusers are not deterred, though, and their attempted abuse must be thwarted by preventives. If the preventives work, the attempt is foiled. If the preventives fail, however, detection is the last screen in attempting to uncover abuses.

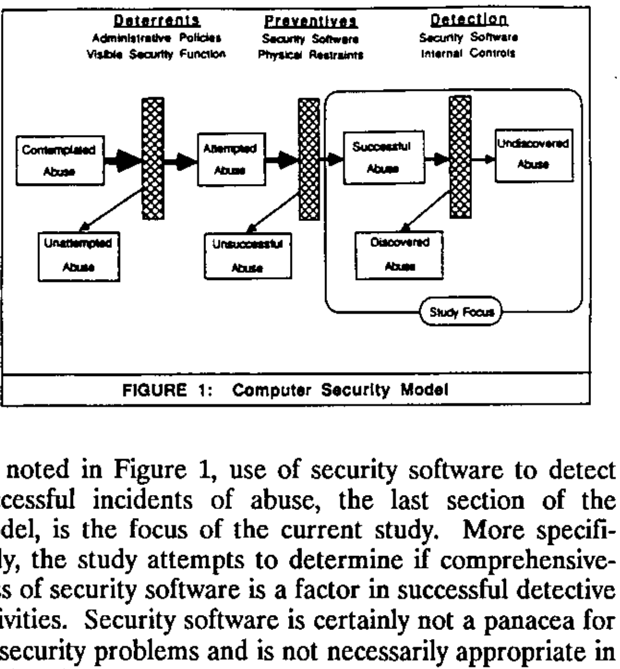

FIGURE 1: Computer Security Model

As noted in Figure 1, use of security software to detect successful incidents of abuse, the last section of the model, is the focus of the current study. More specifically, the study attempts to determine if comprehensiveness of security software is a factor in successful detective activities. Security software is certainly not a panacea for all security problems and is not necessarily appropriate in all situations and for all types of abuse. It may, however, be helpful in improving detection in some settings. Thus, this study attempts to determine the organizational factors associated with use of security software, and to determine the degree to which more sophisticated software improves detection of abuse.

3. TYPES OF SECURITY SOFTWARE

Security software provides both preventive and detective features. *Preventive* software provides "access control," also known as "logical" or "programmed" controls, and may operate at varying levels. Software systems, for example, can limit use to finer and finer "levels of granularity" (Simmons 1984), ranging from applications programs and databases to files, records, and fields (Everest 1986). *Detective* software features are items such as transaction log reports and audit trails used in monitoring and tracking computer use activities (Squillace 1985; Clyde 1987).

The current study uses these characteristics to differentiate "system sophistication" based on the "comprehensiveness" of coverage provided by various types of software. "Low" sophistication operating systems (OS) target security at the level of account and/or database/file access control only; they provide basic recording of violation attempts (Downs 1984). "Mid-level" sophistication database management system (DBMS) and fourth generation language (4GL) packages target access control at finer levels of granularity, specifically records, fields, or statistical summaries; they, too, provide relatively simple records of unauthorized activities (Butterworth 1984; Everest 1986; Van der Lans 1986). At a "high" level of sophistication, specialized security software packages are comprehensive systems providing both a wide range of access control capabilities, plus detailed "tracking" or transaction logs of all activity taking place regarding system activity (Squillace, 1985; Clyde, 1987).

OS-level controls are the predominant type of security software available, with generally optional security features built into nearly all mainframe and minicomputer operating systems. OS-level systems are primarily concerned with file access control, using procedures such as user ID and passwords, designation of read-write-delete-execute capabilities, multiuser restrictions, and data encryption (Cashin 1986; Littman 1984). While focusing primarily on access control, OS security systems may also provide elementary detection features such as access violation logs. These logs note items such as date, time, location, and number of attempted unauthorized accesses.

DBMS and *4GL* systems typically work hand-in-hand, as 4GLs are used to access data stored within DBMSs. Similar to operating systems, DBMS/4GL security features are also optional and primarily concerned with access control. However, DBMSs provide more fine-tuned access controls than operating systems by providing user access to pre-defined portions or "views" of the database, restricting users' ability to update data or modify database structures, and controlling simultaneous access (Van der Lans 1986). With a DBMS configured to provide different users with different views, 4GL queries formulated to retrieve data can be checked against individual users' prespecified access rights. Once again, DBMS/4GL systems are not limited to access control; they too can provide simple detection features reporting attempted unauthorized accesses.

Finally, *specialized software systems* are packages written for the sole purpose of providing security. This is clearly in contrast with OS and DBMS/4GL software where security features are optional and ancillary to the primary function of the software. As with other types of security software, specialized systems provide access and activity restrictions. They are most commonly differentiated from less sophisticated controls, though, by their advanced transaction logging capabilities, which in turn provide complete audit trails (Squillace 1985) and in-depth security violations reports (Clyde 1987). In granting computer security personnel detailed information regarding the use of computer resources, specialized software packages go far beyond simple access control; they can also actively *monitor* and *follow-up* on access violations (Clyde 1987). A plethora of specialized security packages exist. Two widely used systems, both running on IBM equipment, are Resource Access Control Facility (RACF) and Access Control Facility II (ACFII) (Cashin 1986). Many others are also available for both IBM and non-IBM shops.

4. RESEARCH QUESTIONS

This study utilizes two basic constructs for assessing security software installations in organizations, namely the *number* and *sophistication* of systems utilized. As noted earlier, active and visible security functions utilizing a variety of security techniques seem to be a successful deterrent to computer abuse; such organizations can be considered to have more "advanced" security. Within the realm of security software, organizations utilizing both more and more comprehensive systems are considered to be more advanced than organizations with fewer and less sophisticated systems.

The intent of the current study is to attempt to determine organizational factors associated with security software utilization, and to evaluate whether more comprehensive security software is associated with successful abuse detection. To accomplish this objective, the study asks three general research questions:

1. How prevalent is security software in organizations today and what organizational factors are associated with number of systems utilized?

2. How sophisticated is security software used in organizations today and what organizational factors are associated with the sophistication of these systems?

3. What is the nature of the relationship between security software sophistication and discovery of computer abuse incidents?

These research questions address the status of security software from two different perspectives: *quantity* and *quality*. Within each of these questions, several more specific study questions were asked in order to evaluate factors associated with use of security software. Data on prevalence, or quantity of systems used across the sample, increases our understanding of the frequency with which security software is utilized in organizations. Data on sophistication, or quality, helps us to understand factors associated with more or less comprehensive security software. Finally, data on relationships between software sophistication and successful computer abuse detection helps explain relationships between these two constructs.

4.1 Prevalence

How prevalent are security software systems in organizations today and what organizational factors are associated with the number of systems utilized in an organization? The study addresses this question by evaluating whether the number of systems utilized is associated with a variety of organizational factors. The following study questions were asked:

Q1 Is number of security software systems related to organizational size as measured by:

1.1 total assets of the organization at all locations?

1.2 total assets at the respondent's location?

1.3 EDP budget at the respondent's location?

Q2 Is number of security software systems related to type of industry?

Q3 Is number of security software systems related to maturity of the security function?

4.2 Sophistication

How sophisticated are security software systems used in organizations today, and what organizational factors are associated with the sophistication of these systems? To address this question, sophistication of utilized systems was evaluated against the same organizational factors as in the prevalence questions. The following study questions were asked:

Q4 Is security software sophistication related to organizational size as measured by:

4.1 total assets of the organization at all locations?

4.2 total assets at the respondent's location?

4.3 EDP budget at the respondent's location?

Q5 Is security software sophistication related to type of industry?

Q6 Is security software sophistication related to maturity of the security function?

4.3 Discovery of Abuse

What is the nature of the relationship between sophistication of security software systems and discovery of computer abuse incidents? To address this question, sophistication of security software systems was treated as an independent variable and compared with two key aspects of computer abuse incidents: ability to identify perpetrators and seriousness of the abuse (Straub and Nance 1987). As noted earlier, ability to detect abuse may be dependent upon available information detailing unauthorized activities. While OS and DBMS/4GL security features may provide modest recording and reporting capabilities, it is expected that increased detail provided by specialized software reports will facilitate more successful detection. The following study questions were asked:

Q7 Does use of more sophisticated security software increase an organization's ability to identify the perpetrator of computer abuse incidents?

Q8 Does use of more sophisticated security software increase an organization's ability to uncover more serious computer abuse incidents?

4.4 Discussion of Study Questions

As noted earlier, one of the primary objectives of this study is to add to the growing body of knowledge in the field of computer security and abuse deterrence. Toward this end, Q1 and Q4 seek to determine whether associations between organizational size and use of advanced computer security techniques extend into the realm of security software. Larger organizations spend both more time and money on computer security and EDP audit activities than smaller organizations (Straub 1986a); it follows that they would also be more likely to use more comprehensive security software.

Another objective is to identify areas of vulnerability to computer abuse in order to assist security administrators in targeting abuse detection efforts. Q2 and Q5, therefore, examine differences between industries. Some industries are expected to be more vulnerable to computer abuse (e.g., banking, merchandising) and may utilize more comprehensive security techniques to cope with this vulnerability. Individuals responsible for security in industries found to be below average in utilizing security software can be alerted to the situation.

To help understand underlying determinants of advanced security, Q3 and Q6 evaluate whether use of more advanced security software is associated with maturity of the security function. As security staffs gain experience over time, they are exposed to new systems and can be expected to implement a greater number of these systems to handle specific aspects of security. In turn, as exposure to new systems increases, installed systems are likely to be more comprehensive.

Finally, it has been discussed throughout this article that a proactive approach to security is a successful deterrent to computer abuse. Q7 and Q8 assess this relationship in connection with security software. While severity of punishment imposed on perpetrators of abuse has been shown to be a successful deterrent (Straub and Nance 1987), such punishments are predicated upon identification of the perpetrators. Q7 explores the ability of sophisticated software to make such identifications. Similarly, in attempting to target abuse detection activities, discovery of serious abuses should be a major objective. Q8 evaluates whether more comprehensive security software is a useful technique in discovering such incidents.

5. METHODOLOGY

5.1 Data Collection

Data for this study is part of a victimization database obtained in a prior study of computer abuse and deterrent measures (Straub 1986a). The survey instrument (see Appendix) was validated via extensive field interviews with 35 system professionals, interviews and questionnaire responses from a group of 88, and, finally, pilot study responses from 170. A more detailed description of the overall validation process is found in Straub (1986b). The validated survey was mailed out to randomly-selected DPMA (Data Processing Management Association) members in 1986. The sample base that resulted from this study and the pilot group, with duplicates removed, was 1,063.

Of the 1,063 respondents, 528 organizations reported having some level of security commitment, determined by total personnel hours dedicated to computer security exceeding zero (question 12a). These 528 organizations with active security were chosen as the sample base because security software is useful in detecting abuse only to the extent that someone in the organization is actively responsible for responding to reported violation attempts.

Finally, within these 528 organizations, 168 separate incidents of computer abuse were reported. Each incident was accompanied by a separate page containing questions 28-43, addressing various aspects of individual abuse incidents.

5.2 Measures

Prevalence of security software was measured on questions 16 and 17 of the research instrument. Question 16 assessed the number of OS and DBMS/4GL systems by requesting the number of "SECURITY SOFTWARE SYSTEMS available and actively in use on the mainframe(s) or minicomputer(s) at this location." This study used only the number actively in use. Question 17 measured the number of specialized systems by asking the number of "SPECIALIZED SECURITY SOFTWARE SYSTEMS actively in use (examples: ACFII and RACF)."

Sophistication was also measured on questions 16 and 17, as organizations reporting use of multiple system types were collapsed into a single ranked category. In order of sophistication, from least to most comprehensive, the categories were: 1) None, 2) Operating System, 3) DBMS/4GL, and 4) Specialized Software. This collapsing of responses resulted in all organizations being included in one and only one class since organizations were placed in the sophistication category corresponding to their highest ranked system.

By not addressing the number of different types used, this classification scheme is limited. For example, an organization using five separate OS, three DBMS/4GL, and no specialized security software packages was classified as less sophisticated than an organization using a single specialized package and no OS or DBMS/4GL systems. However, since a single specialized system may well provide more extensive security than a multitude of OS and DBMS/4GL systems, this coding scheme probably accurately reflects the comprehensive nature of such systems.

Maturity of the organization's security function was derived from the difference between inauguration of the security function (question 13) and the time of the data collection.

Seriousness of the abuse was measured by question 37, which asked "In your judgement, how serious a breach of security was this incident?" While more objective measures of dollar losses (questions 38 and 39) were available, there is evidence (Straub and Nance 1987; Straub 1986a) that dollar loss is not as valid a measure of abuse seriousness as this subjective measure.

Finally, *identification* of the perpetrator was measured by question 43, a free-format question which read "Please briefly describe the incident and what finally happened to the perpetrators." Based on the responses to this item, which were reasonably complete, successful identification of perpetrators was coded as either yes or no.

5.3 Statistical Techniques

Statistical techniques used to analyze the data included descriptive statistics and various measures of association. Descriptive statistics provide insight into the overall frequency and sophistication of installed systems. Associations between variables were analyzed using Chi-square contingency tables and Kruscal-Wallis tests of significance.

6. DATA ANALYSIS

6.1 Analysis of Prevalence Questions

In answering the first research question, frequency of security software use, 83 percent of the respondent organizations reported having security software "actively in use." Figure 2 shows the percentage of respondent organizations utilizing various types of security software. A surprising 17 percent utilized no security software at all. Seventy-three percent employed security embedded in operating systems software, 47 percent used security embedded in DBMSs and/or 4GLs, and 42 percent used some type of specialized security package.[1]

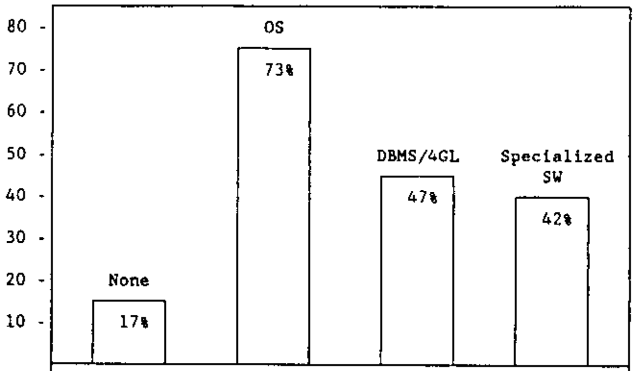

FIGURE 2. Organizational Implementations

Assuming that access control system implementations covary with hardware installations, this usage of OS security measures is to be expected. Virtually all organizations utilizing computers have operating systems security modules, but not all necessarily employ either these OS controls or more sophisticated systems.

Turning to the results[2] of the prevalence questions (Figure 3), several interesting points arise. First, positive relationships between size and prevalence were found. Organizational size, as a broad construct, is clearly associated with the number of security software systems utilized by an organization.

Second, no relationship was found between industry and number of systems. Thus, no conclusions can be drawn about the tendency of one industry to use more or fewer security software systems than any other industry.

Question	Answer
Q1 Is number of security software systems related to organizational size as measured by:	
1.1 total assets of the organization at all locations?	Yes
1.2 total assets at the respondent's location?	Yes
1.3 EDP budget at the respondent's location?	Yes
Q2 Is number of security software systems related to type of industry?	No
Q3 Is number of security software systems related to maturity of the organization's security function?	No

FIGURE 3. Results of Prevalence Questions

Third, no relationship was found between the maturity of the security function and the number of security software systems utilized. This last finding is contrary to expectations. One would expect the number of security systems to increase as the security function ages since maturity of the function would bring increased exposure to security software products and the opportunity to implement new security procedures. One possible explanation of the finding is that rather than simply accumulating new systems, organizations tend to *replace* old systems with new ones. In other words, as they gain experience, organizations may use *better* systems over time.

6.2 Analysis of Sophistication Questions

The second research question addressed the sophistication of security software used in organizations. Figure 4 shows the distribution of organizations based on the sophistication of their security software. Note that the two anchors, "None" and "Specialized Software," contain the same respective proportions of organizations (17 percent and 42 percent) as in the prevalence section above; in fact, they contain the same actual respondent organizations. Collapsing multiple responses from an organization into a sophistication ranking restricts the middle two classifications to organizations which have systems of *no higher sophistication* than that type.

Thus, 17 percent of the respondent organizations utilized *only* operating system security features and another 24 percent used DBMS/4GL systems either in isolation or in combination with OS security features. While 42 percent of the organizations used specialized security software, only 7 percent used such systems in isolation; 35 percent used them in combination with OS and/or DBMS/4GL systems.

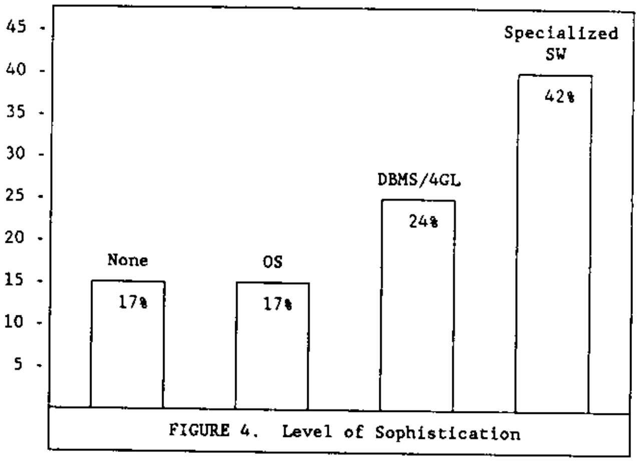

FIGURE 4. Level of Sophistication

The questions on software sophistication (Figure 5) discovered positive relationships between organizational size and sophistication. Larger organizations tend to utilize more sophisticated security software systems than smaller organizations. Thus, as in the prevalence section, organizational size seems to be associated with system sophistication.

Question	Answer
Q4 Is security software sophistication related to organizational size as measured by:	
4.1 total assets of the organization at all locations?	Yes
4.2 total assets at the respondent's location?	Yes
4.3 EDP budget at the respondent's location?	Yes
Q5 Is security software sophistication related to type of industry?	Yes
Q6 Is security software sophistication related to maturity of the organization's security function?	No

FIGURE 5. Results of Sophistication Questions

One major difference between the sophistication and prevalence results was the significant relationship found between industry and sophistication (Q5). In particular, wholesale/retail trade organizations were found to utilize *less sophisticated* systems than expected, while public utilities and manufacturing organizations utilized *more sophisticated* systems.

Once again, no relationship was found between maturity of the security function and security software sophistication (Q6). One would expect that as an EDP shop gains experience and knowledge over time, its expertise would also increase and more comprehensive security tools and techniques would be implemented. Surprisingly, this was not supported; older shops were *not* found to be more likely to use ore sophisticated mechanisms than newer shops. This implies that organizations do not necessarily experience a "learning curve" in implementing security measures, but can implement sophisticated software packages early in the process of developing a security function.

6.3 Analysis of Discovery of Abuse Questions

The final research question addressed the relationship between software sophistication and aspects of abuse discovery. The results of the discovery of abuse questions, shown in Figure 6, indicate that sophistication of security software *is positively related* to discovery of computer abuse.

Question	Answer
Q7 Does use of more sophisticated security software increase an organization's ability to identify the perpetrator of computer abuse incidents?	Yes
Q8 Does use of more sophisticated security software increase an organization's ability to uncover more serious computer abuse incidents?	Yes

FIGURE 6. Results of Discovery of Abuse Incidents Questions

Perpetrators are more likely to be identified and serious losses uncovered when more sophisticated software systems are utilized. Specialized security software provides elaborate security violation reports that identify suspicious user activity and this may lead naturally to discovery of a computer abuser (Q7). Serious abuse incidents also seem to be related to sophisticated software, possibly because users are more aware of the controls and are deterred from abusing the system at more serious levels (Q8). These findings are also in accord with another study (Straub 1986a) which found that prevalence of security software lowered the rate of computer abuse in organizations.

7. DISCUSSION

This study provides insight into the implementation of computer-based control in organizations and raises a number of implications for practitioners responsible for implementing computer security measures. It supports the notion that organizations using "advanced" (i.e., more and better) security software can exercise better control over computer abuse. They can uncover more serious incidents of abuse. They can also unmask more perpetrators.

Currently, larger organizations tend to use more sophisticated software, as do manufacturing and public utility organizations. Wholesale and retail trade organizations, and smaller organizations, utilize *less* sophisticated software. Organizations with less comprehensive security software need to realize that security software can, in the right setting, be effective in addressing the computer abuse threat.

One of the most interesting findings of the study was the lack of association between the maturity of an organization's security function and the number and sophistication of installed security software systems. It suggests that organizations do not necessarily experience a "learning curve" in implementing security measures. Rather, they may be able to introduce advanced software early in the process of developing a security function.

It should be noted that there are significant ramifications of moving rapidly into use of advanced security techniques. On the one hand, young security programs with sophisticated tools may be able to match the level of protection of mature programs without sophisticated tools. On the other hand, introduction of advanced security software into young security environments may backfire (Straub and Hoffer 1988). Unforeseen organizational repercussions could result from the fact that while these systems are more sophisticated and comprehensive, they are also more complex and may strain managerial resources. Moreover, if applied inappropriately, they may be too restrictive and end up causing more problems than they solve.

8. DIRECTIONS FOR FUTURE RESEARCH

The current study is part of an on-going stream of research into computer security and effective countermeasures to the computer abuse threat. Prior studies in this stream have demonstrated that General Deterrence Theory may be a useful starting point for future research since certainty and severity of sanctions imposed on perpetrators of abuse have been found to be successful techniques for curbing abuse. They have also noted the effectiveness of responses such as active security administrators, dissemination of administrative policies and procedures, and internal controls. The current study adds to this growing body of knowledge by demonstrating the usefulness of security software in detecting computer abuse.

While the results here and elsewhere are highly suggestive, more research is still needed. Research on the organizational impacts of security software needs to readdress some of the issues raised in this paper by finding new methods for testing findings, exploring new questions in this general context, and utilizing other theoretical approaches to studying computer abuse.

Regarding methodology, tests triangulating on the phenomenon with different methods are needed to affirm conclusions drawn to date. Security software research calls for in-depth qualitative techniques to give us a fuller understanding of the nature of security administration. Similarly, experimental techniques would increase our understanding of causal relationships.

In addition, other questions need to be asked. For example, how should security software be administered on a day-to-day basis? How does security software impact worker productivity? What other organizational repercussions may occur? These and other relevant areas need further study.

Finally, new theoretical bases may prove useful to subsequent computer abuse research. Sociological theories of deviance, for example, may help explain underlying causes of individuals' abusive behavior. Psychological theories may aid the study of individuals' responses to organizational efforts to reduce abuse. At a broader organizational level, organizational and/or economic risk theories may help explain organizational reluctance to take steps towards implementing security measures.

9. CONCLUSION

While security software does not solve the computer abuse problem, it is a step in the right direction. Computer security techniques need to keep pace with the rising proficiency of computer users. Security software can be an integral part of these activities. Advanced systems provide access restrictions that prevent unauthorized misuse as well as thorough tracking and reporting capabilities for discovering incidents that slip through the preventive net. The current study reinforces a growing awareness that, properly administered, computer security can successfully reduce the threat of computer abuse.

10. REFERENCES

AICPA. "Report on the Study of EDP-Related Fraud in the Banking and Insurance Industries." New York: American Institute of Certified Public Accountants, Inc., Pamphlet, 1984.

Alavi, M., and Weiss, I. "Managing the Risks Associated With End-User Computing." *Journal of Management Information Systems*, Vol. 2, No. 3, Winter 1985, pp. 5-20.

American Bar Association. "Report on Computer Crime." Washington, DC: Task Force on Computer Crime, American Bar Association, Section on Criminal Justice, Pamphlet, 1984.

Brancheau, J., and Wetherbe, J. "Key Issues in Information Systems--1986." *MIS Quarterly*, Vol. 11, No. 1, March 1987, pp. 23-45.

Butterworth, P. "Security-Minded System Design Can Protect Data Bases." *Electronics*, March 8, 1984, pp. 136-140.

Cashin, J. "As Systems Spread Out Data Becomes Vulnerable." *Software News*, December 1986, pp. 40-48.

Clyde, A. "Insider Threat on Automated Information Systems." *Fourth Insider Threat Identification System Conference*, August 1987, Bethesda, MA.

Cohen, J. *Statistical Power Analysis for the Behavioral Sciences*. New York: Academic Press, 1969.

Dickson, G. W.; Leitheiser, R. L.; Wetherbe, J. C.; and Nechis, M. "Key Information Systems Issues for the 80's." *MIS Quarterly*, Vol. 8, No. 3, September 1984, pp. 135-159.

Downs, D. "Operating Systems Key Security with Basic Software Mechanisms." *Electronics*, March 8 1984, pp. 122-127.

Everest, G. *Database Management: Objectives, System Functions, and Administration*. New York, NY: McGraw-Hill, Inc., 1986.

Littman, J. "The Security Challenge." *PC Week*, November 20, 1984, pp. 67-77.

Manuel, T. "Computer Security." *Electronics*, March 8, 1984, p. 121.

Simmons, R. "An Overview of Computer Security." *IBM Systems Journal*, Vol. 23, No. 4, 1984, pp. 309-325.

Sprague, R., and McNurlin, C. (eds.). *Information Systems Management in Practice*. Englewood Cliffs, NJ: Prentice-Hall, 1986.

Squillace, D. "An In-depth Look at IBM's RACF Security System." *Software News*, October 1985, pp. 94-95.

Straub, D. "Deterring Computer Abuse: the Effectiveness of Deterrent Countermeasures in the Computer Security Environment." Unpublished Doctoral Dissertation, Indiana University School of Business, Bloomington, 1986a.

Straub, D. "Instrument Validation in the MIS Research Process." *Proceedings of the Annual Administrative Sciences Association of Canada Conference*, Whistler, British Columbia, June 1-3, 1986b.

Straub, D., and Hoffer, J. "Computer Abuse and Computer Security Administration: A Study of Contemporary Information Security Methods." Bloomington, IN: Indiana University School of Business, Institute for Research on the Management of Information Systems Working Paper #W801, 1988.

Straub, D., and Nance, W. "The Discovery and Prosecution of Computer Abuse: Assessing IS Managerial Responses." Bloomington, IN: Indiana University School of Business, Institute for Research on the Management of Information Systems Working Paper #W708, 1987.

Van der Lans, R. "Data Security in a Relational Database Environment." *Computers & Security*, No. 4, 1986, pp. 128-134.

Walden, J. "Cracking Down on Micro Crime." *Business Computer Systems*, October 1985, pp. 40-56.

11. ENDNOTES

1. Total percentages exceed 100 percent because many organizations reported using more than one type of security software system and were thus included in multiple categories.

2. Due to the exploratory nature of the research, an alpha level of .10 was selected. A "yes" answer, therefore, indicates that the relationship is statistically significant at $p < .10$; a "no" answer indicates that the relationship is not statistically significant. The study's large sample size, moreover, provided power in excess of .97 on all tests. This exceeds the .80 level which Cohen (1969) suggests as sufficient to test medium-sized effects, the pragmatic effects a researcher is usually seeking. As a result, where a relationship was found, there is a high probability than a relationship does, in fact, exist. Similarly, a "no" response indicates that we can state with some confidence that no relationship exists.

APPENDIX

Section I.
Computer Abuse Questionnaire

Personal Information

1. YOUR POSITION:

□ President/Owner/Director/Chairman/Partner
□ Vice President/General Manager
□ Vice President of EDP
□ Director/Manager/Head/Chief of EDP/MIS
□ Director/Manager of Programming
□ Director/Manager of Systems & Procedures
□ Director/Manager of Communications
□ Director/Manager of EDP Operations
□ Director/Manager of Data Administration
□ Director/Manager of Personal Computers
□ Director/Manager of Information Center
□ Data Administrator or Data Base Administrator
□ Data/Computer Security Officer
□ Senior Systems Analyst
□ Systems/Information Analyst
□ Chief/Lead/Senior Applications Programmer
□ Applications Programmer
□ Chief/Lead/Senior Systems Programmer
□ Systems Programmer
□ Chief/Lead/Senior Operator
□ Machine or Computer Operator

□ Vice President of Finance
□ Controller
□ Director/Manager Internal Auditing or EDP Auditing
□ Director/Manager of Plant/Building Security
□ EDP Auditor
□ Internal Auditor
□ Consultant
□ Educator
□ User of EDP
□ Other (please specify): ____________________

2. YOUR IMMEDIATE SUPERVISOR'S POSITION:

□ President/Owner/Director/Chairman/Partner
□ Vice President/General Manager
□ Vice President of EDP
□ Director/Manager/Head/Chief of EDP/MIS
□ Director/Manager of Programming
□ Director/Manager of Systems & Procedures
□ Director/Manager of Communications
□ Director/Manager of EDP Operations
□ Director/Manager of Data Administration
□ Director/Manager of Personal Computers
□ Director/Manager of Information Center
□ Data/Computer Security Officer
□ Senior Systems Analyst
□ Chief/Lead/Senior Applications Programmer
□ Chief/Lead/Senior Systems Programmer
□ Chief/Lead/Senior Machine or Computer Operator

□ Vice President of Finance
□ Controller
□ Director/Manager Internal Auditing or EDP Auditing
□ Director/Manager of Plant/Building Security

□ Other (please specify): ____________________

3. NUMBER OF TOTAL YEARS EXPERIENCE IN/WITH INFORMATION SYSTEMS?

□ More than 14 years
□ 11 to 14 years
□ 7 to 10 years
□ 3 to 6 years
□ Less than 3 years
□ Not sure

Organizational Information

4. Approximate ASSETS and annual REVENUES of your organization:

ASSETS			REVENUES	
At all Locations	At this Location		At all Locations	At this Location
□	□	.... Over 5 Billion	□	□
□	□	...... 1 Billion–5 Billion	□	□
□	□	..... 250 Million–1 Billion	□	□
□	□	... 100 Million–250 Million ...	□	□
□	□	.... 50 Million–100 Million ...	□	□
□	□	.... 10 Million–50 Million	□	□
□	□	..... 5 Million–10 Million	□	□
□	□	..... 2 Million–5 Million	□	□
□	□	...... 1 Million–2 Million	□	□
□	□	...... Under 1 Million	□	□
□	□	.... Not sure	□	□

5. NUMBER OF EMPLOYEES of your organization:

	At all Locations	At this Location
10,000 or more	□	□
5,000–9,999	□	□
2,500–4,999	□	□
1,000–2,499	□	□
750–999	□	□
500–749	□	□
250–499	□	□
100–249	□	□
6–99	□	□
Fewer than 6	□	□
Not sure	□	□

6. PRIMARY END PRODUCT OR SERVICE of your organization at this location:

□ Manufacturing and Processing
□ Chemical or Pharmaceutical
□ Government: Federal, State, Municipal including Military
□ Educational: Colleges, Universities, and other Educational Institutions
□ Computer and Data Processing Services including Software Services, Service Bureaus, Time-Sharing and Consultants
□ Finance: Banking, Insurance, Real Estate, Securities, and Credit
□ Trade: Wholesale and Retail
□ Medical and Legal Services
□ Petroleum
□ Transportation Services: Land, Sea, and Air
□ Utilities: Communications, Electric, Gas, and Sanitary Services
□ Construction, Mining, and Agriculture
□ Other (please specify): ____________________

Are you located at Corporate Headquarters: Yes □ No □

7. CITY (at this location)? __________ STATE? __________

8. TOTAL NUMBER OF EDP (Electronic Data Processing) EMPLOYEES at this location (excluding data input personnel):

□ More than 300
□ 250-300
□ 200-249
□ 150-199
□ 100-149
□ 50-99
□ 10-49
□ Fewer than 10
□ Not sure

9. Approximate EDP BUDGET per year of your organization at this location:

□ Over $20 Million
□ $10-$20 Million
□ $8-$10 Million
□ $6-$8 Million
□ $4-$6 Million
□ $2-$4 Million
□ $1-$2 Million
□ Under $1 Million
□ Not sure

Computer Security, Internal Audit, and Abuse Incident Information

A Computer Security function in an organization is any *purposeful* activity that has the objective of protecting assets such as hardware, programs, data, and computer service from loss or misuse. Examples of personnel engaged in computer security functions include: data security and systems assurance officers. For this questionnaire, computer security and EDP audit functions will be considered separately.

	Computer Security	EDP Audit
10. How many staff members are working 20 hours per week or more in these functions at this location?	___ (number of persons)	___ (number of persons)
11. How many staff members are working 19 hours per week or less in these functions at this location?	___ (number of persons)	___ (number of persons)
12. What are the total personnel hours per week dedicated to these functions?	___ (total hours/wk)	___ (total hours/wk)
13. When were these functions initiated?	__/__ (month/yr)	__/__ (month/yr)

If your answer to the Computer Security part of question 12 was zero, please go directly to question 25. Otherwise, continue.

14. Of these total computer security personnel hours per week (question 12), how many are dedicated to each of the following?

A. Physical security administration, disaster recovery, and contingency planning .... ____ (hours/week)
B. Data security administration .... ____ (hours/week)
C. User and coordinator training .... ____ (hours/week)
D. Other .... ____ (hours/week)
(please specify): ________________

15. EXPENDITURES per year for computer security at this location:

Annual computer security personnel salaries ..... $________

Do you have insurance (separate policy or rider) specifically for computer security losses?
□ Yes □ No □ Not sure

If yes, what is the annual cost of such insurance ... $________

16. SECURITY SOFTWARE SYSTEMS available and actively in use on the mainframe(s) [or minicomputer(s)] at this location:

	Number of available systems?	Number of systems in use?
Operating system access control facilities...	___	___
DBMS security access control facilities	___	___
Fourth Generation software access control facilities	___	___

17. Other than those security software systems you listed in question 16, how many SPECIALIZED SECURITY SOFTWARE SYSTEMS are actively in use? (*Examples: ACF II, RACF*)

____
(number of specialized security software systems actively in use)

Of these, how many were purchased from a vendor? ______
(number purchased from a vendor)

... and how many were developed in-house? ______
(number developed in-house)

18. Through what INFORMATIONAL SOURCES are computer system users made aware OF THE APPROPRIATE AND INAPPROPRIATE USES OF THE COMPUTER SYSTEM?
(Choose as many as applicable)

□ Distributed EDP Guidelines
□ Administrative program to classify information by sensitivity
□ Periodic departmental memos and notes
□ Distributed statements of professional ethics
□ Computer Security Violations Reports
□ Organizational meetings
□ Computer Security Awareness Training sessions
□ Informal discussions
□ Other (please specify): ________________

19. Which types of DISCIPLINARY ACTION do these informational sources mention (question 18) as consequences of purposeful computer abuse?
(Choose as many as applicable)

□ Reprimand
□ Probation or suspension
□ Firing
□ Criminal prosecution
□ Civil prosecution
□ Other (please specify): ________________

In questions 20-24, please indicate your reactions to the following statements:

	Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
20. The current computer security effort was in reaction in large part to actual or suspected past incidents of computer abuse at this location.	□	□	□	□	□
21. The activities of computer security administrators are well known to users at this location.	□	□	□	□	□
22. The presence and activities of computer security administrators deter anyone who might abuse the computer system at this location.	□	□	□	□	□
23. Relative to our type of industry computer security is very effective at this location.	□	□	□	□	□
24. The overall security philosophy at this location is to provide very tight security without hindering productivity.	□	□	□	□	□

25. How many SEPARATE UNAUTHORIZED AND DELIBERATE INCIDENTS OF COMPUTER ABUSE has your organization at this location experienced in the 3 year period, Jan. 1, 1983-Jan. 1, 1986?
________ (number of incidents)

(Please fill out a separate "Computer Abuse Incident Report" [Blue-colored Section II] for each incident.)

26. How many incidents do you have reason to suspect other than those numbered above in this same 3 year period, Jan. 1, 1983-Jan. 1, 1986?
________ (number of suspected incidents)

27. Please briefly describe the basis (bases) for these suspicions.

____
____
____
____

Section II.
Computer Abuse Incident Report

(covering the 3 year period, Jan. 1, 1983-Jan. 1, 1986)

Instructions: Please fill out a separate report for each incident of computer abuse that has occurred in the 3 year period, Jan. 1, 1983-Jan. 1, 1986

28. WHEN WAS THIS INCIDENT DISCOVERED?

Month/year _____/_____

29. HOW MANY PEOPLE WERE INVOLVED in committing the computer abuse in this incident?

_________(number of perpetrators)

30. POSITION(S) OF OFFENDER(S):

	Main Offender	Second Offender
Top executive	□	□
Security officer	□	□
Auditor	□	□
Controller	□	□
Manager, supervisor	□	□
Systems Programmer	□	□
Data entry staff	□	□
Applications Programmer	□	□
Systems analyst	□	□
Machine or computer operator	□	□
Other EDP staff	□	□
Accountant	□	□
Clerical personnel	□	□
Student	□	□
Consultant	□	□
Not sure	□	□
Other	□	□

(please specify): (Main)__________

(Second) __________

31. STATUS(ES) OF OFFENDER(S) when incident occurred:

	Main Offender	Second Offender
Employee	□	□
Ex-employee	□	□
Non-employee	□	□
Not sure	□	□
Other	□	□

(please specify): (Main)__________

(Second) __________

32. MOTIVATION(S) OF OFFENDER(S):

	Main Offender	Second Offender
Ignorance of proper professional conduct	□	□
Personal gain	□	□
Misguided playfulness	□	□
Maliciousness or revenge	□	□
Not sure	□	□
Other	□	□

(please specify): (Main)__________

(Second) __________

33. MAJOR ASSET AFFECTED or involved:
(Choose as many as applicable)
□ Unauthorized use of computer service
□ Disruption of computer service
□ Data
□ Hardware
□ Programs

34. Was this a one-time incident or had it been going on for a period of time? __
(Choose one only)
□ one-time event
□ going on for a period of time
□ not sure

35. If a one-time incident, WHEN DID IT OCCUR?
Month ________ Year ________

36. If the incident had been going on for a period of time how long was that?
________years ________months

37. In your judgment, how serious a breach of security was this incident?
(Choose one only)
□ Extremely serious
□ Serious
□ Of minimal importance
□ Not sure
□ Of negligible importance

38. Estimated $ LOSS through LOST OPPORTUNITIES (if measurable): *(Example: $3,000 in lost business because of data corruption)*

$__________
(estimated $ loss through lost opportunities)

39. Estimated $ LOSS through THEFT and/or RECOVERY COSTS from abuse: *(Example: $12,000 electronically embezzled plus $1,000 in salary to recover from data corruption + $2,000 in legal fees = $15,000)*

$__________
(estimated $ loss through theft and/or recovery costs)

40. This incident was discovered...
(Choose as many as applicable)
□ by accident by a system user
□ by accident by a systems staff member or an internal/EDP auditor
□ through a computer security investigation other than an audit
□ by an internal/EDP audit
□ through normal systems controls, like software or procedural controls
□ by an external audit
□ not sure
□ other (please specify):

____

41. This incident was reported to....
(Choose as many as applicable)
□ someone inside the local organization
□ someone outside the local organization
□ not sure

42. If this incident was reported to someone outside the local organization, who was that?
(Choose as many as applicable)
□ someone at divisional or corporate headquarters
□ the media
□ the police
□ other authorities
□ not sure

43. Please briefly describe the incident and what finally happened to the perpetrator(s).

____
____
____
____
____
____
____
____