1987

CONTROLLING COMPUTER ABUSE: AM EMPIRICAL STUDY OF EFFECTIVE SECURITY COUNTERMEASURES

Detmar W. Straub Jr.
University of Minnesota

CONTROLLING COMPUTER ABUSE: AN EMPIRICAL STUDY OF EFFECTIVE SECURITY COUNTERMEASURES

Detmar W. Straub, Jr.
Management Information Systems
Curtis L. Carlson School of Management
University of Minnesota

ABSTRACT

Considerable evidence has come to light that information systems are vulnerable to dangerously high and persistent abuse and that managers perceive this threat to be high. The organizational response to abusive potential has been to implement a computer security administrative unit with the charge of deterring and preventing computer abuse.

Exactly how effective are the countermeasures employed by these units? This victimization survey of 1,211 randomly selected DPMA organizations has determined that computer abuse can be controlled through a set of deterrent administrative procedures and through preventive security software. Understanding these relationships should greatly assist IS managers in allocating resources to the security function and in disseminating this pertinent information to top management.

INTRODUCTION

This study addresses the problem of computer system security. Its purpose is to ascertain ways in which computer systems are being abused and to assess the effect of current countermeasures on the incidence of computer abuse/crime. For the purposes of this study, computer abuse was defined as an intentional misuse of organizational resources such as computer service, hardware, data, and programs.[1]

As rapidly as technical security measures have been advancing, the potential for large individual losses in the tens of millions of dollars is growing faster still (Parker 1983, 1984). Case histories and sample survey data to date enumerate organizational losses at every point on the impact continuum (AICPA 1984; Colton et al. 1982a, 1982b; Straub 1986a; Whiteside 1978), losses which can rapidly aggregate to a staggering total. The American Bar Association survey (ABA 1984) reports total dollar losses of approximately $.5 billion for 72 firms; a simple projection of this figure to the entire United States business community suggested to the task force that computer abuse was an "enormous" problem in the United States (p. xii). Furthermore, "known and verifiable losses" in this study averaged in the millions of dollars. Although distribution of losses from computer abuse are heavily skewed by large variances (Parker 1976), averages of this size do show the dire potential for large scale thefts by high tech embezzlers. Parker's SRI databank of computer abuse (Parker 1976) cited averages of $500,000 while computer crimes in state and local government appear to average $329,000 (Allen 1977). The extent of the problem is perhaps demonstrated most convincingly in the fact that a large percentage of major U.S. firms (25%) are uncovering serious incidents of abuse each year (ABA 1984).

Future losses from computer abuse could be even more damaging. Anti-social individuals are becoming increasingly proficient in disrupting computer service, stealing data and programs, and creating general havoc in the information systems they have targeted as victims (Lee, Segal and Steier 1986; Straub 1986b; Marbach 1983; Parker 1983, 1976). More disturbing even than this maliciousness are indications that hard core criminal elements are poised to plunder the nation's informational storehouses on a systematic basis (Parker 1983; Conover 1984; Sokolik 1980).

Along with evidence that abuse is taking place nationally at a dangerous rate, information system (IS) managers perceive the problems of computer abuse (and error) to be significant. Computer trade journals and weeklies regularly feature computer security as a topic of interest. Additional compelling evidence for the importance of the subject is indicated by the frequency with which

security and control are cited as a key management issue in opinion surveys of IS managers.

ORGANIZATIONAL RESPONSES TO COMPUTER ABUSE: SECURITY ROLES AND TASKS

Perception of the latent vulnerability of modern computerized systems has led to the slow accretion of specialized computer security units within organizations and the implementation of classes of countermeasures (Straub and Hoffer 1987). About half of the organizations polled in a 1985 survey (Straub 1986a) assigned staff to the administration of computer security on a full or part-time basis. In terms of organizational structure, most of these administrators are situated in the information systems area. Some common titles include "Director of Data Security," "Manager of Computer Security," and "Computer Security Administrator" (Straub 1986a).

Security administrators employ a range of techniques to guard against purposeful or accidental system misuse.[2] Two classes of these countermeasures -- namely, deterrent and preventive countermeasures -- are being evaluated in this study. Deterrents are those essentially passive, administrative controls that take no active role in restricting the use of system resources. Examples include distributed guidelines specifying conditions for proper use of the system and Computer Security Awareness Training Sessions. Preventives, on the other hand, screen access to the system and theoretically admit only authorized users. Locks on computer equipment room doors are examples of physical restraints whereas software locks on accounts, files, transactions, and data items are instances of programmed restraints.

RELEVANT LITERATURE

Exactly how effective have the countermeasures employed by these security units been?[3] Unfortunately, prior studies do not answer questions about the causal linkage between activities of security administrators, their use of security software, and computer abuse. These studies include both victimization surveys (ABA 1984; AICPA 1984; Kusserow 1983 [otherwise known as the PCIE study, for President's Council on Integrity and Efficiency]; Local Government Audit Inspectorate 1981) and archival data gathered from media and police reports of abuse (Parker 1976, 1981). Descriptive statistics presented in prior studies--frequency distributions of abuse by dollar loss category, offender motivation type, and victim industry type -- do address important questions about the phenomenon of computer abuse. But the data has not been tested through cross tabulations nor through more sophisticated techniques such as multivariate or nonparametric tests.

The belief that countermeasures can be implemented to reduce the risk of abuse does appear, however, throughout the abuse literature in the form of authoritative opinion (Sokolik 1980; Madnick 1978). Parker specifically advocates the value of deterrent countermeasures in numerous places in his works (Parker 1981, 1983). Deterrents, such as guidelines and policy statements, are instrumental, he believes, in lowering abuse by white collar amateurs. The purposes of such deterrents are: 1) to clarify exactly what constitutes legitimate use of the information system and 2) to discourage weakly motivated potential offenders by the threat of serious consequences resulting from system misuse (cf. also Gilhooley 1980; Dunn 1982).

Other countermeasures that are believed to have a major effect on abuse include preventive physical and software measures. The most common form of software access control is password protection. Other sophisticated security features that screen for a wide spectrum of conditionalities of use such as time of day, previous unsuccessful logins, etc. have been modelled (Hartson and Hsaio 1976) and are now available in commercial packages.

In sum, there is a considerable body of authoritative opinion about the nature of abuse and circumstances that are thought to minimize it. Soft controls such as policy statements and security awareness training as well as hard controls such as password access controls are believed to be effective against abuse, but no substantive, empirical evidence has been collected to underwrite this opinion. Moreover, even though prior work has measured a host of variables associated with abuse, scientific controls -- internal validities as they are generally understood (Cook and Campbell 1979)-- are missing from these endeavors.

The current study investigates whether computer abuse can be controlled through countermeasures currently being employed by IS security units. In this respect alone, it goes beyond prior studies in the field. Besides using statistical analyses to determine the manner in which variables correlate,

it also attempts to gather more accurate data about the abuse phenomenon by rigorous validation of its research instrument.

RESEARCH QUESTIONS AND OPERATIONAL DEFINITION OF COMPUTER ABUSE

Based on the literature search, two primary research questions have been devised for the study:

- o Are deterrent and preventive countermeasures effective in controlling abuse?
- o What role do other organizational factors play in controlling abuse?

Because of the varying ways in which the term "computer abuse" has been used, the term was restricted in this study to the abuse perpetrated by individuals against organizations (Kling 1980). The working definition presented to study respondents was:

> 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).

GENERAL DETERRENCE THEORY IN THE REFERENCE DISCIPLINE, CRIMINOLOGY

Reference disciplines can serve as a springboard for the application of established knowledge to new fields and emerging technologies (Dickson, Benbasat and King 1980). Examples of articles that demonstrate the intellectual connections between MIS and other disciplines include Kriebel and Moore (1980) and Bariff and Ginzberg (1980).

An obvious reference discipline for activities that involve a violation of social codes is criminology, and this discipline provides a ready behavioral explanation for why deterrents may be effective controls. The most applicable theory, General Deterrence theory, has well established research constructs and causal relationships. There is a long-standing tradition of research in this area and concurrence by panels of experts on the explanatory power of the theory (Blumstein 1978; Cook 1982). Constructs and measures have been developed to test the theory since the early 1960s, and its application to the computer security environment is now timely.

The thrust of most of the theoretic deterrence literature has been on "disincentives" or sanctions against committing a deviant act. Disincentives are traditionally divided into two related but independent, conceptual components: 1) certainty of sanction and 2) severity of sanction (Blumstein 1978). The theory holds that under conditions in which risk of being punished is high and penalties for violation of norms are severe, potential offenders will refrain from illicit behaviors.

In the literature, observable commitment of an enforcement group, such as the police in punishing offenders, typically serves as a surrogate for perception of risk or certainty of sanction (Gibbs 1975). This assumes that potential offenders perceive risk to be in direct proportion to efforts to monitor and uncover illicit behaviors. In other words, people believe that punishment will be more certain when enforcement agents explicitly or implicitly "police," or make their presence felt to potential offenders. In information systems, this is equivalent to security administrators making their presence felt through monitoring, enforcing, and distributing information about the organizational policies regarding system usage, or what we have been referring to as deterrent countermeasures. When punishment is severe, it is assumed that offenders, especially less motivated potential offenders, are dissuaded from antisocial acts (Straub and Widom 1984). Table2 1 presents the pertinent connections between the conceptual terminology we have been using and constructs most frequently cited in General Deterrence theory.

Table 1. Concepts, Constructs, and Measures

Concepts	Research Construct	Survey Item	Measure Description
Abuse	DAMAGE	25	- Number of incidents
		39	- Actual dollar loss
		38	- Opportunity dollar loss
		37	- Subjective seriousness index
Deterrents	DISINCENTIVES: CERTAINTY	10	- Full-time security staff
		11	- Part-time security staff
		12	- Total security hours/week
		14b	- Data security hours/week
		15	- Total security staff salaries
		22	- Subjective deterrent effect
		3-35 & 3-28-36	- Longevity of security (from inception to incident date)
	DISINCENTIVES: SEVERITY	18	- Information about proper use
		19	- Most severe penalty for abuse
		22	- Subjective deterrent effect
Preventives	PREVENTIVES	16	- Use of software access control
		17	- Use of specialized software
Rival Explanations	ENVIRONMENTAL-MOTIVATIONAL FACTORS	30	- Privileged status of offender
		29	- Amount of collusion
		32	- Motivation of offender
		31	- Employee/non-employee status
		24	- Tightness of security
		21	- Visibility of security
		28-35 & 36	- Duration of abuse

General Deterrence theory, moreover, has particular applicability to computer abuse. Especially strong evidence for the efficacy of deterrents in situations similar to computer abuse can be found throughout the literature (cf., for example, Schwartz and Orleans 1967). Computer abuse can be typically characterized as an amateur, white collar act (Sokolik 1980). Because computer abuse takes place in the relatively benign environment of persons who normally abide by rules and regulations (Sokolik 1980), it is believed that sanctions can mitigate misuse of computers. That is, from the perspective of purposeful misuse, most offenders are amateurs. Either out of ignorance or out of a desire for pecuniary gain, they are willing to violate social norms, but are not so strongly motivated that deterrent measures cannot inhibit them (Parker 1981; Straub and Widom 1984).[4]

MODELLING DETERRENT AND PREVENTIVE COUNTERMEASURE

The strong causal link between deterrent disincentives and lower abusive damage are openly stated in General Deterrence theory and in the abuse literature. Moreover, as noted above, the abuse literature argues that preventives are instrumental in curbing abuse. Rival hypotheses were modelled to rule out, wherever possible, other feasible explanations of abusive effects. A parsimonious model of the relationship between cause and effect in computer abuse appears in Figure 1. The three primary causal constructs are represented by labels within circles and causal paths as lines between constructs. For the sake of clarity, the two disincentive constructs have been combined as "Deterrents" in this model. Rival hypotheses were scaled so that higher values in the independent variables would be reflected in higher values in the dependent variables. For example, a large number of high-privileged system users would be expected to increase organizational losses from computer abuse.

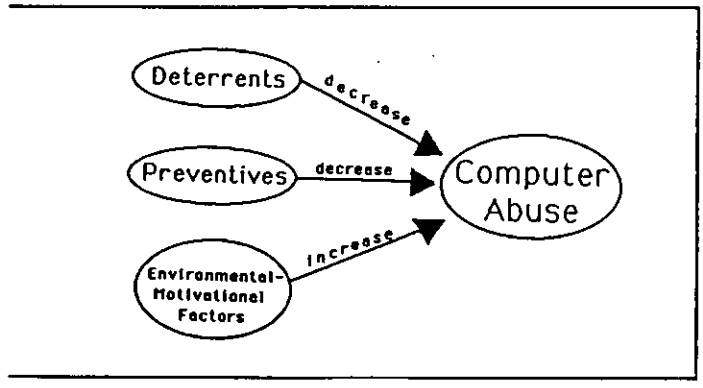

Figure 1. The Security Impact Model

METHODOLOGY

A victimization questionnaire was chosen to determine the structural relationships between countermeasures and computer abuse and to provide the best possible measures of the dependent or endogenous variable, abusive damage (see Appendix for study instrument). Cross-sectional studies in this vein have long served to evaluate causal relationships between correlated variables in criminological investigations (Greenberg and Kessler 1982; Nagin 1978; Dodge, Lentzner and Shenk 1976; Skogan 1981). With modifications tailored for the computer security environment, the victimization survey has given good service in this study.

Variable selection was based on theory, victimization surveys in the criminological field, prior computer abuse instruments, and abuse literature. Theoretically-oriented variables appear in the model as disincentive and damage constructs, constructs which will be used to test General Deterrence

theory. The preventives construct was derived from the abuse literature. The composite environmental-motivational factors serving as the rival hypotheses evolved out of prior computer abuse work and implicit elements of General Deterrence theory. The connection among research concepts, constructs, and measures in the survey are shown graphically in Table 1 and is discussed in much greater detail in Straub (1986b).

Measures for each of the research constructs were devised and validated over the two year period 1984-1985. The instrument was validated via extensive field interviews with 35 system professionals, interviews and questionnaire responses from a group of 88, and, finally, questionnaire responses from 170. This validated survey was mailed out to a group of 5,489 randomly selected DPMA (Data Processing Management Association) members. The sample base that resulted from a final administration of this survey was 1,211 with reports on 259 separate abusive incidents. A more detailed description of the validation process is found in Straub (1986c).

Hypotheses that reflect expected relationships between independent and dependent variables in conceptual and statistical terms are delineated in Figure 2.

Research Hypotheses	Research Questions
Conceptually: H(1): Abusive damage is significantly inhibited by the certainty and severity of punishment for abuse. Statistically: H(1): Damage is not independent of deterrents.	Q(1)
Conceptually: H(2): Abusive damage is significantly inhibited by preventive software. Statistically: H(2): Damage is not independent of preventives.	Q(1)
Conceptually: H(3): Abusive damage is significantly inhibited by environmental-motivational factors. Statistically: H(3): Damage is not independent of the rival hypotheses, environmental-motivational factors.	Q(2)

Figure 2. Research Hypotheses

Statistical techniques chosen for the study, the last methodological component of interest, include (1) LISREL (LInear Structural RELations) modelling and (2) a set of multivariate and univariate correlational tests. These techniques complement each other nicely by providing different quantitative readings on the data. In this study, LISREL was used to initially confirm or disconfirm the explanatory power of disincentives. Additional corroborative tests offer strengths such as distribution-free assumptions (non-parametric tests), zero order or direct effect measures (Chi-Square Contingency Tables), and nonstructural tests of covariance equality (canonical correlation). A more intricate description of the statistical procedures used to analyze this data, and the analyses themselves, may be found in Straub (1986b).

Testing of the abuse data through multiple statistical techniques permits the same data set to be viewed through complementary methodologies, each with its own distinct strengths and weaknesses. Much as multiple operations of constructs and multiple methods of instrumentation help to validate theories about underlying processes (Cook and Campbell 1979), the use of statistical analyses with varying assumptions can grant a more three dimensional perspective on the interactions between data sets. This approach is more robust than a one-technique analysis precisely because it is not heavily dependent on the truth of a single set of assumptions.

DATA ANALYSIS

An initial set of tests for nonresponse bias in the sample data was performed to ensure that respondents did not differ systematically from nonrespondents. Any significant effect in this case would reduce confidence in our ability to generalize findings to the entire population. Results from these tests indicate that nonresponse bias were not present.

The data was next examined for adherence to the Security Impact Model. LISREL analysis showed that the model of deterrent efforts and abusive damage fit reasonably well, i.e., the Security Impact Model fits the actual sample data. Hypothesis 1, therefore, was supported in the analysis. Goodness-of-fit indices (.68) and variance explained (36.6%) are sufficiently large to argue in favor of the explanatory power of the model. Causal coefficients representing the negative effect of deterrents on

damage, moreover, are statistically significant at the .05 level (Straub 1986b).

By means of the confirmatory factor analysis component of LISREL, factor loadings were also estimated in the analysis. For the dependent variables composing the damage construct, loading from the number of incidents measure (Item 25) was heaviest, followed by the subjective estimate of damage (Item 37). Dollar estimates of damage (Items 38 and 39) had low factor loadings. Variables that contributed most to the deterrent and preventive constructs are shown in Table 2.

Table 2. Loadings of Prominent LISREL Causal Factors

Variable	Loading
Disincentives: severity	
Number of informational sources about conduct (Item 18)	29.543
Most severe disciplinary action (Item 19)	23.697
Disincentives: certainty	
Total personnel hours/week (Item 12)	3.400
Data security hours/week (Item 14b)	3.022
Full-time security personnel (Item 10)	2.755
Subjective estimate of deterrent effect (Item 22)	1.000
Preventives	
Number of security software packages in place (Items 16 and 17)	3.078

A LISREL test of the rival hypotheses showed that they helped to improve the model fit and the explained variance. The causal coefficient for the linkage was significant, statistically and practically, and the goodness-of-fit indicators were sufficiently large to support this conclusion. Hypothesis 3, therefore, did receive support in the LISREL analysis. Among the environmental-motivational factors that demonstrated highest loadings were: a) employment status of offender (Item 31), b) motivation of offender (Item 32), and c) position of offender (Item 30).

Additional tests of the causal model were utilized to deepen the analysis. This series of multivariate and univariate corroborative tests confirmed that relationships do exist between theorized variable sets and individual variables within these sets. Canonical correlational analysis detected the presence of direct dependency between deterrents and damage although not between environmental-motivational factors and damage. Nonparametric analyses (Kruscal-Wallis tests and Chi-Square Contingency Table tests) revealed that the majority of variables loading heavily on constructs in the multivariate analysis also demonstrated pairwise links with the number of incidents measure (Item 25); conversely, lightly loading factors in the multivariate analyses generally had no significant links with abusive damage.

Table 3 synthesizes findings from the corroborative analyses as well as the LISREL analysis in a rough-hewn tally form. The major independent variables are listed in order of importance by construct. That is, if a variable was found to be heavily loaded and/or statistically significant at the .05 level, a tally mark appears under the applicable test. Because canonical correlation looks at relationships between sets of variables, the preventives-abuse linkage was not tested in this analysis (Hair et al. 1979).

DISCUSSION

Interpretation of data in a field as new as computer security and abuse is by definition tenuous. Nevertheless, the data does demonstrate patterns which must be taken with some seriousness so that research can push ahead to more clearly specify causal relationships between constructs. This synthesis will attempt to evaluate evidence quantitatively and qualitatively and to provide a balanced view of the findings.

Each statistical technique revealed variant perspectives on variable relationships in the sample. It would be highly unusual -- even to the point of incredulity -- were all test results identical. Some of the selected techniques accommodate the partialling effects of variables on each other while others do not. Some transform the data into ranks and correlations before testing it while others test a form of the data much closer to the raw data.

Table 3. Summary of Prominent Causal Factors

Independent Variable	LISREL Test	Canonical Correlation Test	Kruscal-Wallis Test	Chi Square Test	Total
Deterrents					
Data Security Hours/Week (Item 14b)	X	X	X	X	4
Total Personnel Hours/Week (Item 12)	X	X	X	X	4
Most Severe Disciplinary Action (Item 19)	X	X	X	X	4
Number of informational sources about conduct (Item 18)	X	X	X		3
Subjective Estimate of Deterrent Effect (Item 22)		X	X	X	3
Full-Time Security Personnel (Item 10)	X		X		2
Total Salaries of Security Personnel (Item 15)				X	1
Preventives					
Number of Security Software Packages in Place (Items 16 and 17)	X	—	X	X	3
Environmental-Motivational Factors					
Offender Employment Status (Item 31)	X				1
Motivation of Offender (Item 32)	X				1
Position of Offender (Item 30)	X				1

Given the varieties of ways in which the data has been handled by the statistics, patterns that emerge independent of technique are more robust than with single analytical treatments.

It should be noted first that deterrents and abusive damage proved to be related as predicted by General Deterrence theory, and, specifically, research hypothesis 1. Both the LISREL and canonical correlational analyses showed these effects; and General Deterrence theory received distinct, though not unanimous support in the nonparametric analyses. As rival hypotheses, environmental-motivational factors received support only in the LISREL analysis.

Security countermeasures, as measured through data security hours and total hours, stand out as generic causal factors in all tests. This has been maintained by security specialists for a long time and thus the argument that general deterrence works in the computer security environment now has some tentative support. Duties of security officers often include disseminating information about proper system usage and penalties for abusing systems. These too appear as causal factors in the data.

According to the data, abuse may also be prevented by means of security software. The more extensive the security imposed at various system levels--from the file level down to the data item level--the less vulnerable is the system to abuse. Preventives and deterrents that consistently emerge in the data analysis are:

- o Data security hours
- o Overall security hours
- o Information about proper system usage
- o Penalties for violations
- o Security software

DIRECTIONS FOR FURTHER RESEARCH AND IMPLICATIONS FOR PRACTICE

Very likely, there are other explanations for patterns of abuse in organizations. The presence of deterrents and preventives do explain lower abuse to some degree, but industry type and size of EDP shop also appear to have explanatory power (Straub and Hoffer 1987). Motivations, such as maliciousness, greed, opportunity, and incentive, may explain a part of abusive behavior as well. Further tests will help to unveil these underlying patterns.

Overall study findings reveal that General Deterrence theory can be successfully applied to the computer security environment. These findings need triangulation through studies employing stronger internal validity checks, such as field and laboratory experimentation. In this vein, a field experiment testing the effect of strong and weak deterrence in the academic environment has already been completed. Replication in a business setting at some future time can round out this initial set of field tests.

Because of the strong theoretical connection between potential offender attitudes and abuse, laboratory studies might also advance our knowledge. In criminological studies, seriousness indices commonly serve to measure initial impressions about perceived risk and severity of punishment in particular situations. An experimental deterrent treatment which simulates a Computer Security Awareness Training session could test for lower post-treatment indices. In addition, qualitative research techniques, field interviews and case studies, can provide variant perspectives.

The major implication of this study for the administration of computer security is straightforward: security appears to be effective. An active and visible security staff and a commitment to data security figure prominently in this formulation, as do control activities in which security staff inform users about improper system usage and penalties for noncompliance. Security software also helps to curb computer abuse.

As managers increasingly come to treat computer abuse as a behavioral and people problem rather than just a technical one, the function of security administration is gradually being incorporated into the life stream of American business. This evolution is occurring slowly in certain industrial groups. Given the findings of this study, these industries need to reevaluate their position vis-a-vis security and seriously consider initiating, strengthening, or modifying security efforts in their firms.

ENDNOTES

[1] It is well known that controls designed to protect against deliberate acts can also be useful in preventing unintentional acts. This study, however, only deals with intentional, or marginally intentional, acts.

[2] Corrective or recovery measures are also part of the security administrator's repertoire. However, these measures allow the commission of an abuse or error.

[3] Of course, it is not possible to prove directly that an action has *not* taken place because of the absence of deterrents. In this situation, however, criminologists *infer* the effectiveness of deterrents by correlating deterrents with measures of criminal activity.

[4] The incidence of abuse as a result of misunderstandings between management and employees is undoubtedly very high (Straub and Hoffer 1987).

REFERENCES

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

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

Allen, B. "The Biggest Computer Frauds: Lessons for CPAs." *Journal of Accountancy*, Vol. 143, No. 5, May 1977, 53-63.

Bariff, M. L., and Ginzberg M. J. "MIS and the Behavioral Sciences." In E. R. McLean (ed.), *Proceedings of the First International Conference on Information Systems*, December 8-10, 1980, Philadelphia, PA, 49-58.

Blumstein, Alfred. "Introduction." In A. Blumstein, J. Cohen, and D.Nagin (eds), *Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates*, National Academy of Sciences, Washington, DC, 1978.

Colton, K. W.; Tien, J. M.; Davis, S. T.; Dunn, B.; and Barnett, A. I. *Computer Crime: Electronic Fund Transfer Systems and Crime*. U.S. Department of Justice, Bureau of Justice Statistics, Washington, DC, 1982a.

Colton, K. W.; Tien, J. M.; Davis, S. T.; Dunn, B.; and Barnett, A. I. "Electronic Funds Transfer Systems and Crime." Interim Report in on-going study on "The Nature and Extent of Criminal Activity in Electronic Funds Transfer and Electronic Mail Systems," supported by Grant No. 80-BJ-CX-0026, U.S. Bureau of Justice Statistics, 1982b. Referenced by special permission.

Conover, P. "The Year of Computer Illiteracy." *Business Computer Systems*, January 1984.

Cook, P. J. "Research in Criminal Deterrence: Laying the Groundwork for the Second Decade." In *Crime and Justice: An Annual Review of Research*, Vol. 2., The University of Chicago Press, Chicago, 1982, 211-268.

Cook, T. D., and Campbell, D. T. *Quasi-Experimentation: Design and Analytical Issues for Field Settings*. Rand McNally, Chicago, 1979.

Dickson, G. W.; Benbasat, I.; and King, W. R. "The Management Information Systems Area: Problems, Challenges, and Opportunities." In E. R. McLean (ed.), *Proceedings of the First International*

Conference on Information Systems, December 8-10, 1980, Philadelphia, PA, 1-8.

Dodge, R. W.; Lentzner, H. R.; and Shenk, F. "Crime in the United States: A Report on the National Crime Survey." In Wesley G. Skogan, *Sample Surveys of the Victims of Crime*, Ballinger, Cambridge, MA, 1976.

Dunn, T. S. "Methodology for the Optimization of Resources in the Detection of Computer Fraud." Unpublished doctoral dissertation, University of Arizona, 1982.

Gibbs, J. *Crime, Punishment, and Deterrence.* Elsevier, New York, 1975.

Gilhooley, I. A. "Data Security." In *Advances in Computer Security Management*, Heyden, Philadelphia, 1980, 33-55.

Greenberg, D. F., and Kessler, R. C. "Model Specification in Dynamic Analyses of Crime Deterrence." In J. Hagan (ed.), *Deterrence Reconsidered: Methodological Innovations*, Sage, Beverly Hills, CA, 1982.

Hair, J. F., Jr.; Anderson, R. E.; Tatham, R. L.; and Grablowsky, B. J. *Multivariate Data Analysis.* PPC Books, Tulsa, OK, 1979.

Hartson, H. R., and Hsaio, D. K. "Full Protection Specifications in the Semantic Model for Database Protection Languages." *Proceedings of the Annual Conference of the ACM*, Houston, October 1979, 90-95.

Kling, R. "Computer Abuse and Computer Crime as Organizational Activities." *Computer Law Journal*, Vol. 2, No. 2, 1980, 186-196.

Kriebel, C. H., and Moore, J. H. "Economics and Management Information Systems." In E. R. McLean (ed.), *Proceedings of the First International Conference on Information Systems*, December 8-10, 1980, Philadelphia, PA, 19-31.

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

Lee, J. A. N.; Segal, G.; and Steier, R. "Positive Alternatives: A Report on the ACM Panel on Hacking." *Communications of the ACM*, Vol. 29, No. 4, April 1986, 297-299.

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

Madnick, S. "Management Policies and Procedures Needed for Effective Computer Security." *Sloan Management Review*, Fall 1978, 61-74.

Marbach, W. D. "Beware: Hackers at Play." *Newsweek*, 5 September 1983, 42-48.

Nagin, D. "General Deterrence: A Review of the Empirical Evidence." In A. Blumstein, J. Cohen, and D. Nagin (eds), *Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates*, National Academy of Sciences, Washington, DC, 1978.

Parker, D. B. *Crime by Computer.* Scribner's, New York, 1976.

Parker, D. B. *Computer Security Management.* Reston, Reston, VA, 1981.

Parker, D. B. *Fighting Computer Crime.* Scribner's, New York, 1984.

Parker, D. B. Discussant on PBS program, "The Computer Chronicles," aired the week of April 1, 1984.

Schwartz, R. D., and Orleans, S. "On Legal Sanctions." *University of Chicago Law Review*, Vol. 34, Winter 1967, 274-300.

Skogan, W. G. *Issues in the Measurement of Victimization.* NCJ-74682. U.S. Department of Justice, Bureau of Justice Statistics, Washington, DC, 1981.

Sokolik, S. L. "Computer Crime -- The Need for Deterrent Legislation." *Computer/Law Journal*, Vol. 2, No. 2, Spring 1980, 354-382.

Straub, D. W. "Computer Abuse and Computer Security: Update on an Empirical Study." *Security, Audit, and Control Review*, ACM Special Interest Group journal, Vol. 4, No. 2, Spring 1986a, 21-31.

Straub, D. W. "Deterring Computer Abuse: The Effectiveness of Deterrent Countermeasures in the Computer Security Environment." Unpublished doctoral dissertation, Indiana University School of Business, Bloomington, IN, 1986b.

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

Straub, D. W., and Hoffer, J. A. "Computer Abuse and Computer Security: An Empirical Study of Contemporary Information Security Systems." IRMIS (Institute for Research on the Management of Information Systems, Indiana University School of Business, Bloomington, IN, 1987. Discussion Paper.

Straub, D. W., and Widom, C. S. "Deviancy by Bits and Bytes: Computer Abusers and Control Measures." In J. H. Finch and E. G. Dougall (eds.), *Computer Security: A Global Challenge*, Elsevier Science Publishers B.V. (North-Holland) and IFIP, Amsterdam, 1984, 91-102.

Whiteside, T. *Computer Capers*. New American Library, New York, 1978.

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: At all Locations	ASSETS: At this Location		REVENUES: At all Locations	REVENUES: 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 ☐

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).

_____

_____

_____

_____

_____

_____

_____

_____

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: ACFII, 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.

_____

_____

_____

_____