

Effective IS Security

by Detmar W. Straub Jr.

Assistant Professor of MIS
Information and Decision Sciences Dept.
Curtis L. Carlson School of Management
University of Minnesota
271 19th Avenue South
Minneapolis, MN 55455
(612) 625-1012
BITNET: DSTRAUB@UMNACVX

January 16, 1990

Working Paper

**Published as: Straub, Detmar W., "Effective IS Security: An Empirical Study,"
Information Systems Research, 1, 3, (1990), 255-276.**

Copyright © Detmar W. Straub
All rights reserved.

Effective IS Security

A B S T R A C T

Security has not been one of the top issues facing IS managers. Many managers permit their installations to be either lightly protected or wholly unprotected, apparently willing to risk major losses from computer abuse. This study, based on the criminological theory of General Deterrence, investigates whether a management decision to invest in IS security results in more effective control of computer abuse. Data gathered through a survey of 1211 randomly-selected organizations indicates that security countermeasures that include deterrent administrative procedures and preventive security software will result in lower computer abuse. Knowledge about these relationships is useful for making important decisions about the security function.

Post Hoc Observations by the Author on this 1991 Paper

Detmar W. Straub Jr.

J. Mack Robinson Distinguished Professor of Information Systems and Director of Research and Doctoral Programs
Computer Information Systems Department and Electronic Commerce Institute
Robinson College of Business, Georgia State University
Atlanta, GA 30302-4015
email: dstraub@gsu.edu
URL: www.cis.gsu.edu/~dstraub/resume.html
Telephone: (404) 651-3827 (direct); (404) 651-3880 (office)

December, 2000

While the results of this work are probably still credible in the year 2000, certain observations must first be made in order to fully understand (and believe) this assertion. The LISREL tests were performed in 1985-86, when the use of such techniques was still fairly new. By modern standards the paper's AGFIs are low,¹ not "moderate," as it argues. Moreover, whereas the gamma in Figure 5b looks like it should be a beta coefficient, two other linkages in the original model (from motivational-environmental factors to deterrents and to preventives) were removed for parsimony in the course of the editorial process, and the result of this change means that this gamma demarcation is, in fact, accurate (the other insignificant paths were not reported in the published article).² In short, the model presented was a more parsimonious model, but the remaining path indicators leave the impression that the model is not correctly labeled for what was run.

That being said, the LISREL model fit is still not sufficiently good by modern standards to warrant presentation and consideration. Fortunately, three alternative statistical techniques were utilized to test the strength of the overall relationships. As argued in the tally of some of these results in Table 4, deterrents prove to be persuasive antecedents, as predicted by General Deterrence Theory. Preventives also prove to be reasonably good explanators. Rival hypotheses are generally not well supported.

¹See Gefen, David, Detmar Straub and Marie Boudreau, "Structural Equation Modeling Techniques and Regression: Guidelines for Research Practice," *Communications of AIS* (7: 7, August), 2000, 1-78.

² Straub, Detmar W., "Deterring Computer Abuse: the Effectiveness of Deterrent Countermeasures in the Computer Security Environment," unpublished dissertation, Indiana University Graduate School of Business, 1986.

1. Introduction

Over the last several decades, managers have become aware that information and information systems are critical organizational resources. One might assume, therefore, that the **security** of information and information systems would also be seen in a favorable light. In fact, security receives little managerial attention. By 1986, security administration had evolved into a separate functional unit in only about 60% of all organizations (Hoffer and Straub, 1989), suggesting that many of these lightly protected or wholly unprotected installations are willing to risk major losses from computer abuse or accidental disaster. Although the function is appropriately positioned in the Information Systems (IS) Department in most organizations (Straub, 1988), security officers typically report to lower level IS managers rather than to senior managers. This secondary status of security is also reflected in opinion surveys of IS managers who consistently rank security and control in the second decile of critical issues (Ball and Harris, 1982; Dickson et al., 1984; Brancheau and Wetherbe, 1987).³

Numerous explanations have been advanced for this relatively low managerial interest in security. Goodhue and Straub (1989) theorize that managerial concern over security is a function of risk inherent in the industry and actions already taken to secure systems. If so, the low managerial interest that we are seeing would suggest that IS managers perceive their risk to be low. But another explanation for why security resources have been so constrained is that managers have differing attitudes (Goodhue and Straub, 1989) on whether IS security does, in fact, create a better protected and more secure environment.

To what extent, then, does a management investment in security result in lower risk from computer abuse? This study attempts to address this question by looking at losses from intentional system misuse and their link to security countermeasures

³The one exception to this second decile ranking was in Hartlog and Herbert's (1986) results where it ranked sixth.

frequently used to deter and prevent abuse. The constructs of deterrence and prevention are drawn from the criminological theory of General Deterrence.

Data gathered through a survey of 1211 randomly-selected organizations indicates that IS security can reduce computer abuse through countermeasures that include both deterrents and preventive software. Findings indicate that increased security in general results in significantly less damage from intentional abuse. They also show that ***data security*** activities (i.e., electronic as opposed to physical security measures) are an integral factor in managing the risk from abuse. These results of the study suggest that those organizations currently without an IS security function (up to 40 percent of IS Departments [Hoffer and Straub, 1989]) may want to reconsider their security posture and realign priorities to allocate resources to this area.

2. Relevant Literature

Prior studies, which include surveys of the victims of computer abuse (Ernst and Whinney, 1989; ABA, 1984; AICPA, 1984; Kusserow, 1983; Wong, 1985), archival data gathered from media and police reports of abuse (Parker, 1976, 1981), and surveys of prosecutors' offices (BloomBecker, 1986), have not studied causal relationships between the activities of security administrators and computer abuse. Descriptive statistics in prior studies such as frequency distributions of computer abuse by dollar loss, offender motivation, and victim industry have addressed important questions about the phenomenon of computer abuse, but they have not tested relationships among variables.

A number of conceptual studies, however, have hypothesized about the effectiveness of security countermeasures in reducing the risk of computer abuse

(Madnick, 1978; Martin, 1973). Parker (1981, 1983), for example, advocates the value of **deterrents** such as guidelines and policy statements in lowering abuse by white-collar amateurs. Deterrents clarify what constitutes legitimate use of the information system and discourage weakly-motivated potential offenders (Dunn, 1982). Lack of deterrents, on the other hand, leads to a misunderstanding of acceptable system use (Klete, 1975).

Among the **rival explanations** for low levels of computer abuse are countermeasures known as **preventives**. Classes of preventives include physical security of facilities as well as security software (Hsaio et al., 1979). One well known form of security software, for example, would be password protection (Friedman, 1988).

Additionally, rival explanations include certain **motivational factors** which encourage potential abusers to commit computer abuse. One of these factors is occupational role or degree of system privilege. It is thought that the impunity of highly-privileged system users, such as system programmers, EDP auditors, security officers, and top executives, encourages them to engage in large scale computer abuse (Parker, 1981). The literature also suggests that strongly-motivated abusers will commit more damage than weakly motivated abusers (Chambliss, 1967) and that employees, because of their privileged position, will cause more damage than non-employees (Lee et al., 1986). Another factor that is believed to increase damage from computer abuse is perpetrator collusion. Parker (1976, 1981) proposes that larger losses with collusion occur because offenders reinforce each other's actions.

Finally, **environmental factors**, such as the tightness of the security environment and visibility of security administrators, may correlate negatively with computer abuse (Parker, 1981). Tightly controlled environments with highly visible security staff are thought to result in be less frequent and less severe computer abuse.

3. Study Background

To address issues raised in the literature, two primary research questions were posed for this study:

Q(1): Has IS Security been effective in lowering computer abuse through deterrents?

Q(2): Can rival explanations, including use of preventive security software, explain lower incidence of computer abuse?

Because of the varying ways the term "computer abuse" has been used and the need for researchers to limit the scope of their investigations (Taber, 1980), the term was restricted to abuse perpetrated by individuals (or groups of individuals) against organizations (Kling, 1980). The definition of computer abuse used in the study was:

"the unauthorized and deliberate misuse of assets of the local organizational information system by individuals, including violations against:

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

4. Theoretical Base: General Deterrence Theory

The foundation for this study is the criminological theory of General Deterrence. The long tradition of research in this area has well-established research constructs, well-

specified causal relationships, and high consensus among experts on the explanatory power of the theory (Blumstein et al., 1978; Cook, 1982). A corollary economic theory supporting General Deterrence theory was proposed by Ehrlich (1973) and verified by Vandaele (1978). Recent work in the area has further supported this theory.⁴

Deterrence theory focuses on "disincentives" or sanctions against committing a deviant act and the effect of these sanctions on deterring others from committing criminal acts (Blumstein et al., 1978). Disincentives are represented by two sub-constructs: 1) certainty of sanction, and 2) severity of sanction (Blumstein et al., 1978). When the risk of punishment is high (deterrent certainty) and penalties for violation are severe (deterrent severity), the theory predicts that potential offenders will be inhibited from committing anti-social acts.⁵

The theory assumes that potential violators become aware of efforts to control anti-social behaviors. In short, it is assumed that people respond to "policing" and the punishment that is associated with effective policing. In IS, the comparable "policing" activity occurs when, for instance, security officers use deterrents to monitor and enforce policy and distribute information about organizational guidelines for acceptable system usage. Severe penalties for security violations are thought to dissuade potential

⁴See Richards and Tittle (1982) and Tittle (1980) for support of the theory. Richards and Tittle (1982) conclude that "most results [using perceptual risk measures] have proven consistent with the deterrent argument." Paternoster et al., 1982b, found support for a reciprocal relationship between deterrence and anti-social acts, a finding which still partially supports General Deterrence. The most recent evidence of the widespread acceptance of General Deterrence theory is the prominent place it takes in Pearson and Weiner's (1985) integrative theoretical model of criminology.

⁵ Ehrlich's (1973) corollary economic theory of anti-social acts offers support for General Deterrence theory. Ehrlich proposes that these acts emanate from a rational analysis of benefits and costs in which the desirability of the illegitimate activities outweighs risk of sanction. An econometric model of expected gains exceeding expected costs at the margin (a subjective utility function) was tested by means of aggregate data on police expenditures and crime rates. Moreover, Ehrlich's conclusion that this form of General Deterrence theory does explain variations in rates of felonies over time was reinforced by Vandaele's (1978) reexamination of Ehrlich's data.

offenders, especially less motivated potential offenders, from illicit behaviors (Straub and Widom, 1984).⁶

4.1 Modelling Deterrents and Rival Explanations

Figure 1 models the theoretical relationship between deterrents and computer abuse. In this model the deterrents construct is the "summative unit" represented by behavioral "properties" (Dubin, 1978, pp. 66-67) such as IS security efforts. As in the deterrence research, properties of deterrents serve as surrogates for the way security deters potential abusers. Deterrents operationalize how potential abusers perceive risk, i.e, serve as surrogates for risk (Blumstein et al., 1978). The computer abuse construct represents losses from security breaches.

[Figure 1 about here]

The relationship between rival explanations and computer abuse was also modelled. Use of security software, for example, is predicted to be negatively related to losses from computer abuse. Because motivational and environmental factors are thought to influence how much computer abuse occurs, these too were modelled.

Although Figure 1 does not indicate a reverse causal relationship between computer abuse and deterrents, reciprocal effects are a possibility. Numerous studies (e.g., Paternoster et al., 1982a) have linked increased levels of crime to subsequent

⁶Strong evidence for the efficacy of deterrents in situations similar to computer abuse can be found throughout the criminological literature (Schwartz and Orleans, 1967). Computer abuse, as a typical amateur, white-collar act (Sokolik, 1980), takes place in the relatively benign environment of persons who normally abide by rules and regulations (Sokolik, 1980). It is believed, therefore, that sanctions can mitigate misuse of computers. Out of ignorance or a desire for pecuniary gain, they are willing to violate social norms; however, they are not strongly motivated, and deterrent measures can inhibit them (Silberman, 1976).

increases in police activity. It is important, therefore, to investigate such effects (Cook, 1982) in the current study.

5. Instrument Validation

A victimization questionnaire was selected to examine the linkages between deterrents, rival explanations, and computer abuse (see Appendix for validated instrument).⁷ Cross-sectional surveys have long served to evaluate causal relationships in criminology (Greenberg and Kessler, 1982); therefore, a victimization questionnaire modified for the computer security environment was felt to be appropriate for this study. Questionnaire measures were based on theory, victimization surveys in criminology, and previous computer abuse surveys. Measures were devised and tested in three phases over a two-year period. The questionnaire was tested for content validity, construct validity, and reliability.

During the first phase, a draft questionnaire instrument was pre-tested by means of personal interviews. Interviewees included academic experts in research methodology, criminologists, IS practitioners and auditors, and state and local law enforcement officers. The 37 participants, drawn from public and private sector organizations including banking, insurance, manufacturing, trade, utilities, transportation, education, and medical services, made an expert assessment of the content of the draft instrument (Cronbach, 1971). Participants held diverse

⁷ Victimization questionnaires are used widely in criminological studies to test theoretical relationships (Skogan, 1981). The National Crime Survey (NCS) carried out by the Bureau of Justice Statistics is one example. Methodologically, victimization surveys attempt to gather data about crime by polling victims rather than perpetrators of crime. It does gather information about victims and non-victims alike, however (Skogan, 1981).

organizational positions, including CEOs, IS managers, operations supervisors, information security officers, database administrators, and internal auditors.⁸

The second phase employed both interviews and questionnaires. Interviews were conducted in 44 organizations with security officers, IS managers, and internal auditors. In each organization, a parallel questionnaire seeking identical information was administered to a different, but equally-knowledgeable informant (primarily IS managers and internal auditors). Responses from these maximally dissimilar data gathering methods were correlated using Campbell and Fiske's (1959) multitrait-multimethod (MTMM) analysis. Analysis of the MTMM matrix found generally acceptable construct validity, i.e., low method variance and high convergent/discriminant validity. The instrument also included equivalent, maximally similar measures (Campbell, 1960, p. 550) to gauge the extent of the random error (reliability). The instrument demonstrated high internal consistency with Cronbach alphas of .80 or more (Nunally, 1967).

In the third phase, additional tests of validity and reliability were carried out through a pilot survey of 1000 randomly-selected DPMA (Data Processing Management Association) members. One hundred and seventy questionnaires were returned. To

⁸ An issue having to do with both construct validity and reliability, but not precisely either, is whether the respondents were reporting merely on their perceptions of abusive incidents, i.e., a subjective understanding of the phenomenon, or on objective facts about such incidents. There are two reasons for believing that these two forms of measurement were not significantly different in this particular situation. First, there is the evidence from the Phase II validation, which involved responses from two independent, but equally knowledgeable sources of information about computer abuse from each organization. Not only was there substantial agreement on the dimension of losses, but also on the number of incidents (over 75 percent of the incidents were reported by both respondents). In effect, by virtue of the validation procedure itself, measures of key dependent variables, regardless of source, may be said to be accurate, that is "equal and symmetrical" (Campbell and Fiske, 1959). The second reason in favor of the validity of the measures is that during the pretest study participants were asked to verify through company documents, memos, etc. their memory of abusive events. In each case where such documentation existed, objective facts as recorded at the time of the incident did not differ substantively from the respondents' recall of events, in the researcher's opinion.

assess construct validity, principal components factor analysis was used (Allen and Yen, 1979). Key measures of the deterrents construct (number of full-time security staff, part-time staff, total staff hours per week, and staff salaries) loaded heavily on a single factor. After four extractions with eigenvalues of at least 1.0 (Nunnally, 1967), the factor structure accounted for 97 percent of the variance in the dataset. Calculation of Cronbach alphas for the deterrent measures revealed values of .94, .93, .98, and .94, which were acceptable by the .80 standard (Nunally, 1967).

The three phases of instrument validation demonstrated that the research instrument had reasonably good content validity, construct validity, and reliable measures.

6. Operationalization of Constructs

The validated instrument measured all three constructs in the Security Impact model (Figure 1). Table 1 shows the final measures for deterrents, rival explanations, and computer abuse that were used in this research. The following subsections discuss operationalizations of the research constructs.

[Table 1 about here]

6.1 Computer Abuse Construct

Computer abuse was measured by 3 quantitative items: total number of incidents (item 25); theft, replacement, recovery, and legal costs (item 39); and opportunity losses or revenues lost due to the unavailability of system resources (item 38). A fourth subjective measure was a seriousness index of the breach (item 37). This measure is especially useful whenever actual and opportunity losses are trivial but the victim

believes intangible losses (e.g., credibility of system security) are significant (ABA, 1984; Straub, 1986).

6.2 Deterrents Constructs

Deterrent certainty was measured by 7 items, including number of full-time security staff (item 10), part-time staff (item 11), total staff hours per week (item 12), data security hours per week (item 14b), and salaries of security staff (item 15). Deterrent certainty also uses a measure of the success of the security effort, derived from the elapsed months between the inception of security efforts and the occurrence of the abuse (item 13 less item 35 **or** item 13 less item 28 less item 36). In essence, this derived value measures the age of the security operation at the time the abuse first occurs. Contrasting with hours IS security devoted to physical security (item 14a) is data security hours per week (item 14b). Data security, hence, measures the expected security response to high levels of electronic computer abuse in the environment. A subjective estimate of the effectiveness of the local security group to deter abuse (item 22) was included as an alternate method of measuring the construct (Cook and Campbell, 1979).

Deterrent severity was measured by 3 items, namely severity of disciplinary actions (item 19) and number of informational sources about penalties and acceptable system use (item 18). Both of these measures are traditionally used for deterrent severity in criminological research (Cook, 1982). As with deterrent certainty, a subjective measure of the deterrent effect was used to enhance the operationalization (item 22).

6.3 Preventives Construct

Preventives were measured by 2 items, including number of operating system and database (DBMS) security programs in use (item 16) and number of specialized security programs in use (item 17). When security software is used, fewer abuses are expected both because of the direct effect of preventing computer abuse and the indirect effect of deterring computer abuse.

6.4 Motivational and Environmental Factors Construct

These factors were measured by 4 motivational and 3 environmental factors. Offender motivation (item 32), amount of collusion (item 29), and offender employment status (item 31) model **motivations** of perpetrators. 'Offender motivation' discriminates between presumed strength of motivation, ranging from weak incentives, such as ignorance of proper professional conduct, to strong incentives, such as maliciousness or revenge. Highly motivated abusers like saboteurs are believed to be unresponsive to deterrents in situations in which first-time embezzlers would be deterred (Straub and Widom, 1984). As with item 29 'amount of collusion,' the proclivity to abuse should be stronger among colluders than among individuals working alone (Parker, 1976, 1981). The most highly-motivated perpetrators of abuse have been found to be those with the greatest knowledge of the victim's vulnerabilities. Item 31, hence, captures this motivation through the employee/non-employee status of the offender. The final motivational factor is duration of abuse (item 28 less item 35 **or** item 36). Duration of abuse is important because strength of motivation may be related to the length of time an offender or offenders have been engaged in computer abuse (Parker, 1981).

Therefore, the longer an abuse remains undiscovered and offenders are psychologically committed, the less likely that deterrents will have an effect.

Environment can also impact perceptions about the riskiness of illicit ventures. It is widely believed that system risk is a function of the number of computer users assigned high system privileges to read and alter data and programs (Parker, 1981). On the questionnaire, offender position (item 30) gauges the privileged status of those who have abused systems. The final two indicators of the security environment are subjective. Item 24 calls for an evaluation of the overall security philosophy of the organization. Another measure, item 21, assesses the visibility of security staff within the systems environment. It is thought that IS security that manifests its presence by seeking out and prosecuting abuse and by imposing harsh sanctions will immediately affect the perceptions of potential offenders (Buikhuisen, 1974).

7. The Survey Sample

The validated survey was mailed out to a group of 5489 randomly-selected DPMA members. Among the 1211 usable questionnaires returned were reports of 259 separate computer abuse incidents.

7.1 Respondent, Organizational, and Computer Abuse Characteristics

Survey respondents fell into five general categories. As Figure 2 shows, the largest group of respondents was IS Directors. Middle IS managers and top management made up two other groups while a fourth group had official responsibility or special interest in security (IS security officers, controllers or auditors). A fifth group labelled "Other" was comprised of CEOs, CFOs, programmers, analysts, etc. The

sample polled a higher percentage of managers (about 75 percent) than is characteristic of the DPMA membership as a whole (approximately 50 percent). This differential response rate was expected since many of the issues in the questionnaire are related to managerial concerns for controlling and protecting system assets.

[Figure 2 about here]

Table 2 and Figure 3 show a breakdown of the sample by industrial type and size. Table 2 indicates that the survey polled diverse organizational types and sizes. This table also suggests that the IS security function is less widely implemented in industries like medical and legal services than in industries like finance and utilities. Among organizations that have implemented IS security, the number of hours dedicated to security varied from 9.0 hours per week for small IS departments, to 20.3 for medium-sized IS departments, to 94.4 for large IS departments. The distribution of IS department size (Figure 3a) shows that large (100+ employees) and medium-sized (50-99 employees) IS departments are represented by 55 percent of the sample although small departments constitute the single largest group. Total revenues of the sampled organizations (Figure 3b) indicate that large (\$1B+) and medium-sized (\$50M-\$1B) organizations constitute 55 percent of the total sample.

[Table 2 and Figure 3 about here]

Figure 4 shows the distribution of direct losses, such as recovery costs, as well as indirect losses, such as legal fees. As reported in other computer abuse surveys, the distribution is skewed toward a large number of relatively small losses (Parker, 1976). Nevertheless, it is important to note that 8 percent of those who reported dollar loss figures indicate losses in the \$100,000 plus category.

[Figure 4 about here]

7.2 Tests for Non-Response Bias

Tests for non-response bias were performed to ensure that respondents did not differ systematically from non-respondents. Two quantitative tests were performed. The first tested for differences between the group to whom surveys were mailed (the mailed group) and the group who returned the surveys (the respondent group). The second compared time-dated waves of respondents.

The mailed group and the respondent group were compared on the basis of the geographic characteristics of city and region, particularly appropriate comparisons in the case of computer abuse. Parker (1976) has argued that geographic distribution of the data needs to be carefully examined lest sampling techniques disproportionately stress the experience of heavily populated regions. For this analysis, the Chi-Square Goodness-of-Fit Test was employed (Siegel and Castellan, 1988). The results of the Chi-Square tests reveal that no significant differences between the mailed group and the respondent group exist at the .05 level.⁹

It was possible to compare waves of respondents as a result of a follow-up inducement letter sent out six weeks after the survey itself. One hundred and eighty-nine responses received two weeks or more after the inducement letter were coded as the post-inducement wave. These returns served as a surrogate for the non-respondents (Babbie, 1973).

⁹Because of the anonymous nature of the questionnaire, city and state were the only common data elements on the mailed and respondent lists. Regions used were: Northeast, Mid-Atlantic, South-Atlantic, Midwest, South, and West. Since DPMA membership is heavily concentrated in the Midwest, East and North, the regional classifications were distributed accordingly. The seven major cities were likewise chosen to reflect heaviest concentrations of DPMA membership. They were: Chicago, Indianapolis, New York, Atlanta, Miami, Boston, and St. Louis.

Time-dated waves were compared on key demographic and causal measures. These key measures were: total years of information systems experience (item 3), IS budget per year (item 9), total security hours per week (item 12), and number of abuse incidents (item 25). These measures were chosen because they gather key information on participants, organizations, systems, and abuse. If non-respondents differ from respondents on any of these dimensions, the respondents may not be representative of the population.

Table 3 shows the results of the Mann-Whitney U tests. In each instance, p-values were not statistically significant at the .05 level. These results suggest that the study findings can be generalized to the mailed sample of 5489, and, because of the random selection, to the entire DPMA population of 36,000.

[Table 3 about here]

Despite these quantitative tests, non-response bias could still be present. To assure that the sample was not biased, qualitative evidence was gathered. During pretesting of the instrument, the researcher queried each interviewee on his or her likelihood of responding to an anonymous computer abuse survey sponsored by DPMA. The reasons cited for non-response included lack of time, lack of interest, and lack of incentive. Not one respondent indicated he or she would decline to participate because of possible public exposure of internal abuse problems, which is a systematic difference that would adversely impact the dependent variables.¹⁰ In addition, those who indicated they would not respond did not share common traits such as lack of an IS security function, a systematic response that would affect key independent variables.

¹⁰The traditional terms "dependent variable" and "independent variable" are used in this paper to refer either to the set of measures that are, taken together, effects or causes, or individual measures that stand for an effect or a cause.

8. Results

Statistical techniques chosen for the study included *LI*near *ST*ructural *REL*ations modelling (LISREL) and multivariate and univariate correlational tests. LISREL was used to investigate the simultaneous effects of deterrents and rival explanations. The additional corroborative tests offered strengths such as nonstructural tests of covariance equality (canonical correlation), distribution-free tests (Kruskal-Wallis), and zero-order or direct-effect tests (Chi-Square Contingency Tables).

8.1 LISREL Modelling

The Security Impact Model (Figure 1) was tested using the LISREL statistical package. Observed values for measures were entered as were parameters (constraints) specifying causal relationships between constructs. The LISREL package uses confirmatory factor analysis to generate loadings that best describe the specified relationships between measures and constructs. Through structural equations, LISREL then generates causal coefficients that best model the fit between constructs.¹¹

LISREL offers several advantages over other multivariate techniques. First, LISREL can be used to test relationships between constructs that have been measured in multiple ways (Bagozzi, 1980). In regression, on the other hand, measures of the same construct cannot be handled separately within the same linear model (Bielby and Hauser, 1977). LISREL is also superior to multivariate techniques in permitting complicated causal relationships to be expressed through hierarchical or non-hierarchical and recursive or non-recursive structural equations (Blalock, 1969).

¹¹ Causal coefficients in LISREL are similar to betas in regression and may be interpreted in a like manner.

Since intricate causal networks often characterize real world processes, this capability for mathematical modelling is useful both for development of theory (Blalock, 1969) and practical applications (Dubin, 1978). Finally, unlike other multivariate techniques, ordinal and interval data can be handled with equal facility by the LISREL program. For ordinal data, polychloric distributions are generated from the data and a range specified by the researcher (Joreskog and Sorbom, 1983).¹²

LISREL statistical assumptions seem to be reasonable for this dataset. LISREL assumes that 1) error terms between constructs and measures are uncorrelated, 2) error terms of observed values are uncorrelated across structural equations, and 3) the observed values are multinormal in their distributions. LISREL's ability to separate common from unique variance means that the first assumption is tenable. Given the independence of traits from methods revealed in the MTMM instrument validation analysis, the second assumption also appears to be reasonable. Since departures from multinormality affect only the standard errors of the causal coefficients and because parameter estimates in LISREL are consistent (Joreskog and Sorbom, 1983), the large sample size achieved in this study means that the third assumption is also reasonable.

Finally, because LISREL models need to be just-identified or over-identified to ensure that estimates are meaningful in LISREL (Long, 1983), tests for identifiability were run. These tests, including a test of the determinant of the information matrix generated by LISREL (Joreskog and Sorbom, 1983) and a test for necessary or rank condition (Long, 1983), confirmed that the Security Impact model shown in Figure 1 was identifiable.

¹²Intervals between ranked data points do not have to be equally distributed, as in interval-scaled data. If one assumes that the distances between these points are, on the whole, randomly distributed, statistical tests can be performed on the data. Polychloric distributions, therefore, are the distributions against which the differences between ranks can be checked.

8.1.1 LISREL Model Fit

LISREL analysis indicates that the Security Impact Model fits the actual sample data. Figure 5a shows causal coefficients for the linkages between deterrents and computer abuse. β_1 (-.786) and β_2 (-1.572) were significant at the .05 level. The model fits the covariance in the data moderately well, as demonstrated by a goodness of fit index of .680 with an adjusted goodness of fit of .597, where 1.00 is a perfect fit. Perhaps more revealing is that the model has a squared multiple correlation of .366, which may be interpreted to mean that the model accounts for 36.6 percent of the variance in the dataset. It is clear, moreover, that deterrent severity has greater explanatory power than deterrent certainty, as their respective standardized coefficients, -.587 and -.107, indicate.

In a second LISREL model testing the rival explanations (Figure 5b), causal coefficients ($\beta_1 = -.856$; $\beta_2 = -1.56$; $\gamma = -.444$) were all significant at the .05 level.¹³ The model goodness-of-fit index of .692 (adjusted goodness-of-fit = .610) and the squared multiple correlation of .374 (or 37.4 percent explained variance) also support the explanatory power of the model. This model fit was superior to the "deterrents only" model as indicated by an improvement of 20.34 in Chi-Square from the first to the second model, larger than the one degree of freedom lost by estimating the additional parameter.

[Figure 5 about here]

¹³The indirect effects of the environmental-motivational factors construct on deterrents (and thereafter on computer abuse) were also modelled. These gammas of -.052 and .030 were not significant at the .05 level. Given the heterogeneous nature of the environmental-motivational factors construct, this finding is not terribly surprising. One likely explanation for this lack of effect is that the overall impact of the construct is being dampened by several measures only weakly related to deterrents. In short, the construct components may be misspecified.

The improvement in the adjusted goodness-of-fit from .597 to .610 is more meaningful than change in the other indices because the unadjusted goodness-of-fit and the squared multiple correlation always increase with relaxation of fixed parameters (Joreskog and Sorbom, 1983). This outcome is roughly equivalent to the inevitable rise in R-square in regression analysis when variables are added to the linear model. By chance alone, more variance will be accounted for by adding variables or, in this case, by relaxing constraints.

8.1.2 LISREL Tests for Reciprocal Causal Effects

Among those who had experienced incidents within the last three years, nine percent of the reported incidents occurred before security was initiated. The possibility of a reverse causal linkage was therefore considered. One measure of the strength of deterrent certainty is the elapsed time between the inception of the security unit and the abusive incident. When the abusive incident occurred before the inception of security, the derived value of this measure will be negative. In the LISREL estimation procedure, the factor loading will be dampened if the effect is pervasive and its sign will be negative. Since the loading on this factor was not negative, we may infer that the effect of computer abuses on the creation of new IS security units did not counterbalance the deterrent effect posited in the Security Impact model.

To further test for a reverse causal linkage, LISREL analysis was performed on an alternative model. The beta for a reciprocal effect was not significant at the .05 level, however. Again, this result is not surprising given the small number of organizations in this sample which did initiate security during the three years after an incident.

In spite of these results, there is some evidence in the descriptive data that organizations may have **strengthened** security as the result of an abusive incident. A relatively large group of respondents (22.7 percent) reported that their current security effort was primarily the result of past computer abuses (item 20).

8.2 Canonical Correlation Tests

The relationship between deterrents and computer abuse was also tested using canonical correlations. This technique tests the independence of the covariance structures of two sets of measures (Hair et al., 1979) by maximizing the correlation between linear components of sets of measures. For the linkage between deterrent and abuse measures, loadings were significant at the .05 level. The square of the canonical correlation for this set (.51) yields a shared variance of the two sets of 25.6 percent (Figure 6a). Since the test is bidirectional, this means that the covariance in the deterrents set accounts for 25.6 percent of the covariance in the computer abuse set of measures or vice versa. To estimate the simple and unidirectional effect of deterrents on computer abuse, a redundancy index was calculated (Hair et al., 1979), yielding a value of .242. Deterrents, therefore, account for 24.2 percent of the variance in computer abuse.¹⁴

[Figure 6 about here]

Another causal test was the canonical correlation between rival explanations and computer abuse. As shown in Figure 6b, this test indicated that rival explanations were not canonically correlated with computer abuse (p-value = .79). Thus rival explanations did not account for a significant portion of the variance in computer abuse.

¹⁴This also means that the data does not show a statistically significant reciprocal effect of computer abuse on disincentives, i.e., the creation of I/S security units as a result of abuse.

8.3 Additional Corroborative Tests

To further test the Security Impact model, two kinds of nonparametric tests were performed. Kruskal-Wallis One Way Analysis and Chi-Square Contingency Tables were performed on pairs of measures that included one independent variable and one dependent variable. Ten heavily loading independent variables, such as number of informational sources (item 18), were paired with the heavily loading dependent variables number of incidents measure (item 25).¹⁵

Table 4 summarizes the results of all analyses in tally form. The major independent variables are listed in order of importance by construct. That is, if a statistical test found an independent variable to be related to computer abuse at the .05 level, a tally mark appears under the applicable test. P-values for nonparametric tests are indicated also.

[Table 4 about here]

Overall, General Deterrence theory is confirmed by these nonparametric tests. Of the twelve individual tests performed on deterrents as independent variable and computer abuse as dependent variable, ten were significant. Rival explanations, with the exception of preventives, were insignificant in six out of six tests.

9. Discussion and Implications for Practice

As predicted by General Deterrence theory, nearly all tests suggest that IS security deterrents result in reduced incidence of computer abuse. Both the LISREL and

¹⁵To verify that results were not capitalizing on chance, three lightly loading factors were paired with heavily loading factors and ten randomly selected pairs of IVs and DVs were paired. None of these pairs were significant at the .05 level.

canonical correlation analyses confirmed this relationship. Additional support for General Deterrence theory was found using nonparametric analyses. Tests of a reverse causal linkage, however, were not significant, indicating that deterrents do result in lower abuse. Rival explanations of computer abuse, moreover, were generally insignificant. In rank order, deterrents and preventives that proved effective for IS security (cf. Table 4) were 1) weekly hours dedicated to **data security**, 2) overall weekly hours dedicated to security, 3) use of multiple methods to disseminate information about penalties and acceptable system usage, 4) statements of penalties for violations, and 5) use of security software.

In practical terms, several actions should be taken on the basis of the research results. First, policies regarding proper and improper use of the information system need to be established. The more detailed these policies are, the greater the deterrent impact on unacceptable system use. A policy, for example, which specifies that employees sign a data "contract" gives employees responsibility and accountability for certain data.

After policies are in place, IS security officers should inform and educate users about acceptable system use. This information can be communicated in employee orientation sessions or in other settings, and IS security officers should stress that computer abusers will be punished according to the severity of the violation. File trespassing may only invoke a reprimand, but purposeful destruction or modification of critical company data may be grounds for dismissal and subsequent legal action.

Next, with clear cut guidelines in place, IS security officers can strengthen ongoing **data security** efforts such as assigning and monitoring of passwords, classification of data and programs by security level, and surveillance of suspicious

activities on the system. Followup of all identified violations will deter potential abusers and encourage compliance with security directives.

Finally, since results suggest that computer abuse can be prevented by use of security software, IS security officers should consider implementation of software preventives. This software includes operating system security, DBMS security, and specialized security packages such as ACF-II, RACF, and Top Secret.

10. Study Limitations and Directions for Further Research

In spite of the methodological precautions taken in the study, study results may still be debatable. For example, there may be incentives for certain categories of respondents not to respond or the instrument may be defective even though it has been validated. Other explanations may exist for patterns of abuse in organizations, moreover. The employment of deterrents and preventives by IS security explains lower abuse to some extent, but industry type and size of local IS department also appear to have explanatory power (Straub and Hoffer, 1987). Strong motivations, such as maliciousness, greed, opportunity, and incentive, may also explain abusive behavior.

Multiple statistical techniques were used to offset the biases of individual tests, but it is still possible that findings are artifactual. While multivariate techniques such as LISREL and canonical correlation weigh multiple measures of constructs, they also assume that the underlying model is well specified. If the model is not well specified, the techniques will still converge on a best fit which may, in fact, have significant causal coefficients. In this regard these techniques are similar to regression and other multivariate techniques.

The use of LISREL and canonical correlation, moreover, represents a model-fitting approach to research rather than traditional hypothesis testing. Model-fitting seeks to identify combinations of weighted measures leading to the **best possible** correlation between the measures being examined, which is a different approach to the use of statistics than is commonly found in the literature. Findings based on such model-fitting approaches may be capitalizing on chance factors.

Alternative research methodologies can help determine if the results reported here accurately portray the impact of IS security. By using different approaches to study a phenomenon, we can test whether findings hold across methods, times, and settings (Cook and Campbell, 1979). Among the possible new directions for research are studies that employ stronger checks for internal validity, such as field and laboratory experiments.¹⁶ Because of a possible linkage between potential offender attitudes and abuse, laboratory studies might also be undertaken. An experimental deterrent treatment that simulates a Computer Security Awareness Training session could test for lower post-treatment abuse. In addition, qualitative research techniques, field interviews, and case studies, will enhance our perspective.

11. Conclusions

The major implication of this study for the administration of computer security is straightforward: IS security is effective. An active security staff and a commitment to data security are effective controls as are activities in which security staff inform users about unacceptable system use and penalties for noncompliance. Organizations that

¹⁶In this vein, a field experiment testing the effect of strong and weak deterrence in the academic environment has already been completed by the author with results that support General Deterrence theory.

articulate their policy on computer abuse and actively enforce this policy should benefit from these activities. Security measures such as computer security awareness training sessions also reduce losses from abuse.

Security software likewise helps to curb computer abuse, a finding now corroborated by other studies in the field (Nance and Straub, 1988). When system users become aware that IS security is actively monitoring their system activity and that security software can alert security personnel to violations, the deterrent impact on future abuse should be significant.

Figure 1. The Security Impact Model

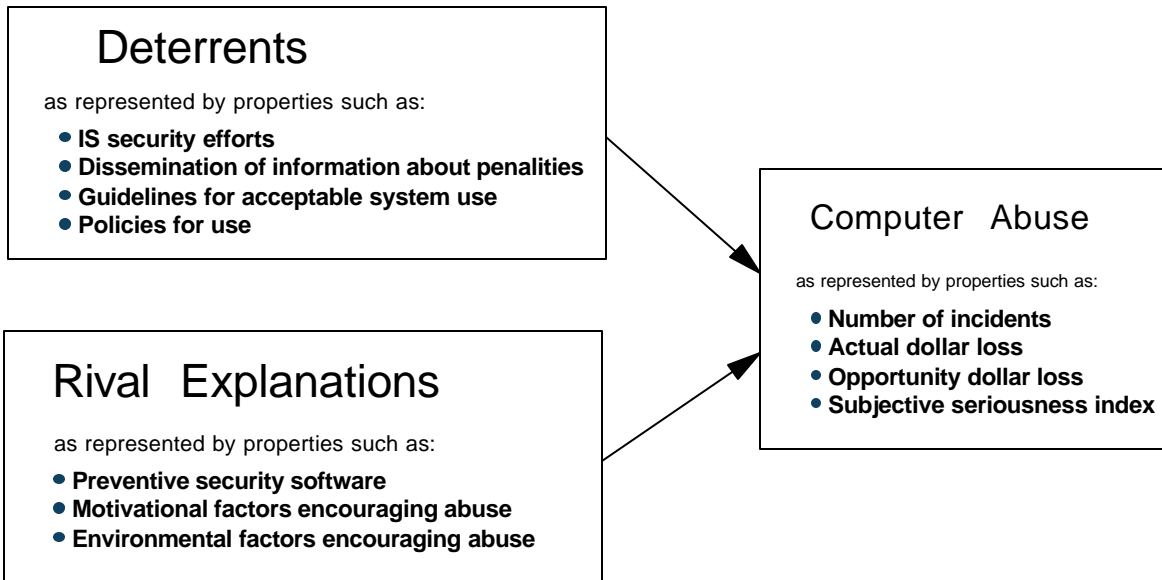


Table 1. Concepts, Constructs, and Measures

Concepts	Constructs	Survey items	Measure Description
Computer abuse	Computer abuse	25 39 38 37	<ul style="list-style-type: none"> ● Number of incidents ● Actual dollar loss ● Opportunity dollar loss ● Subjective seriousness index
Deterrents	Deterrent certainty	10 11 12 14b 15 22 (13-35) or (13-28-36)	<ul style="list-style-type: none"> ● No. of full-time security staff ● No. of part-time security staff ● Total security hours per week ● Data security hours per week ● Total security staff salaries ● Subjective estimate of deterrent effect ● Age of security (elapsed time from inception to incident)
	Deterrent severity	19 18 22	<ul style="list-style-type: none"> ● Severity of penalties for abuse ● No. of informational sources ● Subjective estimate of deterrent effect
Rival Explanations	Preventives	16 17	<ul style="list-style-type: none"> ● No. of OS and DBMS security programs ● No. of specialized security programs
	Motivational Factors	30 32 29 31 (28-35) or 36	<ul style="list-style-type: none"> ● System privilege of offender ● Motivation of offender ● Amount of collusion ● Employee/nonemployee status ● Duration of abuse
	Environmental Factors	24 21	<ul style="list-style-type: none"> ● Environmental tightness of security ● Environmental visibility of security

Table 2. Industry Subsamples and Extent of I/S Security

	N	Percent with No Security
Medical/Legal Servs.	45	62
Construction	29	55
Trade	110	53
Transportation	28	52
Petroleum	14	50
Manufacturing	285	47
Financial Institut.	147	36
Education	93	34
Government	106	34
Data Process. Servs.	105	33
Chemical/Pharmaceut.	60	33
Utilities	54	33

Figure 2. Makeup of Sample Respondents

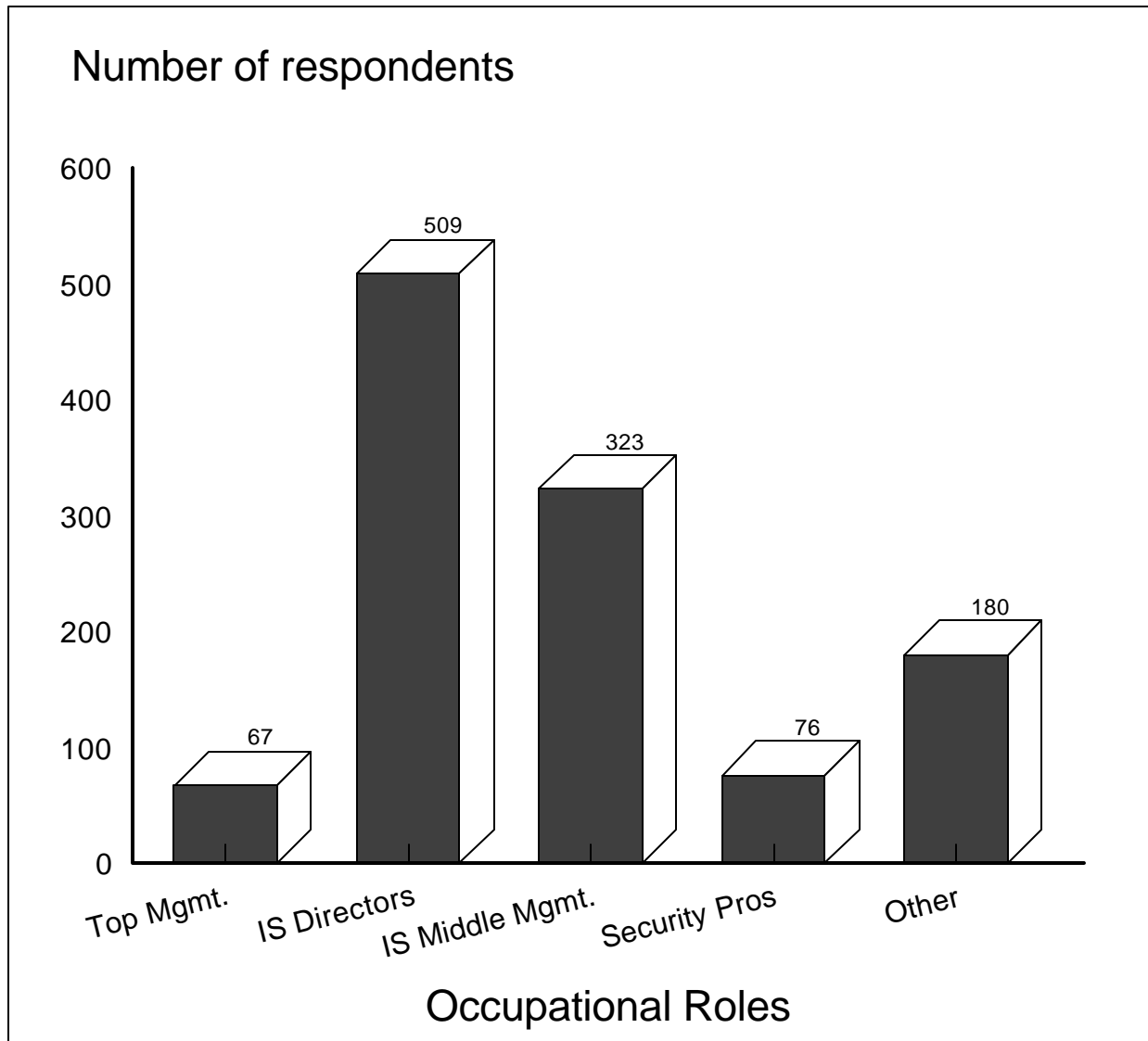


Figure 3. Respondent Size Characteristics

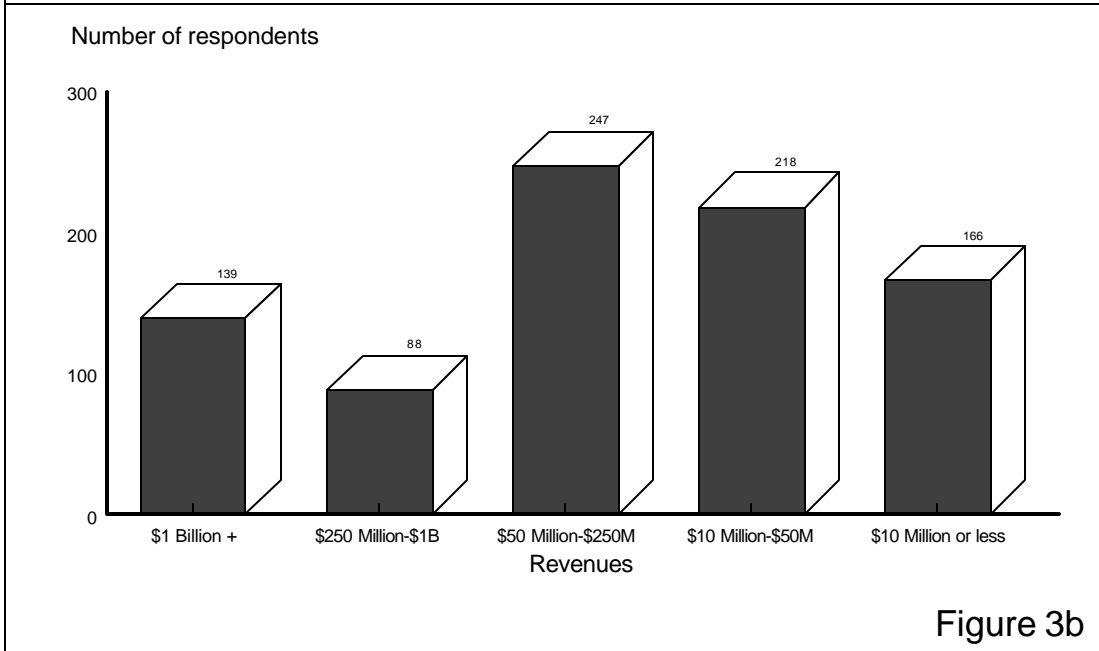
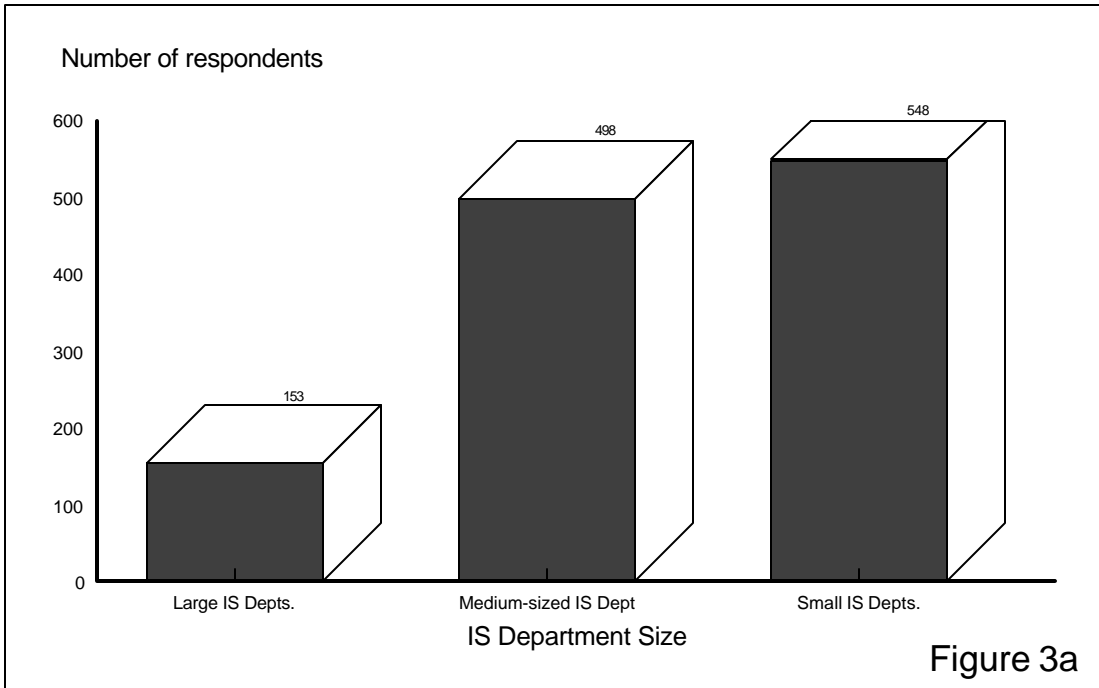
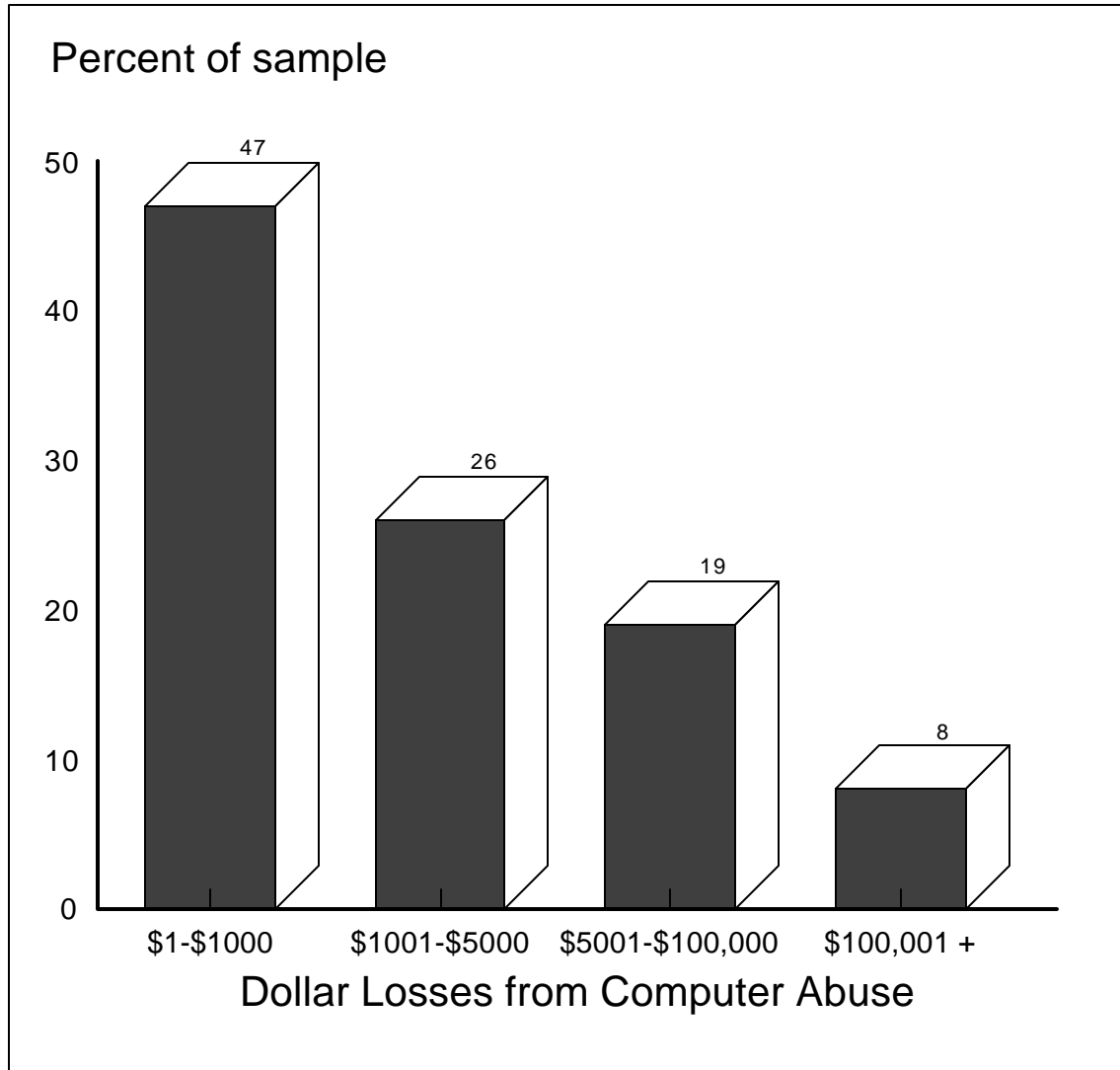


Figure 4. Distribution of Reported Losses



Survey Item	Wave	N***	2-tailed p-value
IS experience (Item 3)	Pre* Post**	544 157	.9484
EDP budget (Item 9)	Pre Post	523 121	.6375
Total security hours (Item 12)	Pre Post	564 147	.2718
Number of Abuses (Item 25)	Pre Post	551 158	.2669
	* Pre-inducement wave		
	** Post-inducement wave		
	*** N in each category (with no missing values)		

Table 3. Mann-Whitney U Tests for Non-Response Bias

Figure 5. LISREL Testing of the Security Impact Model

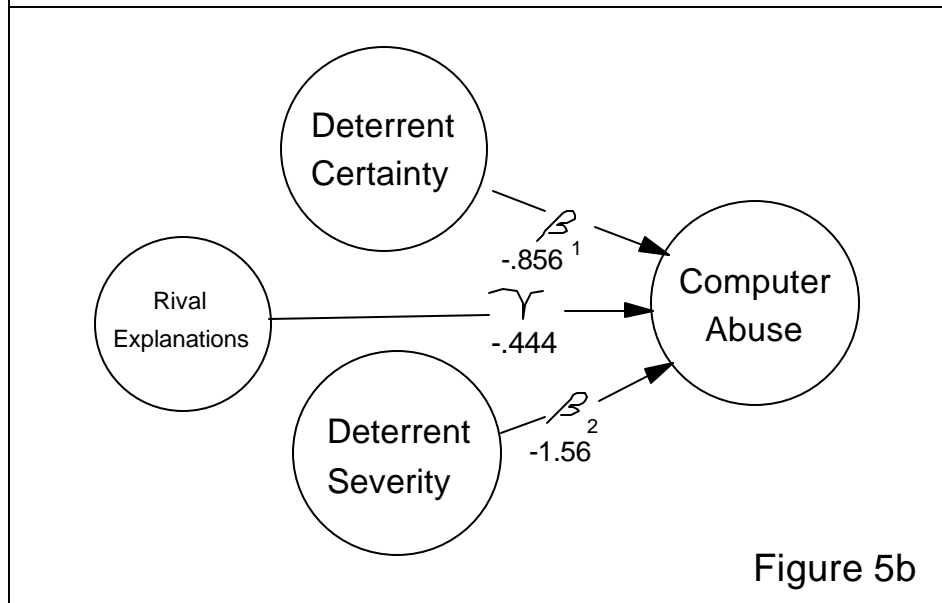
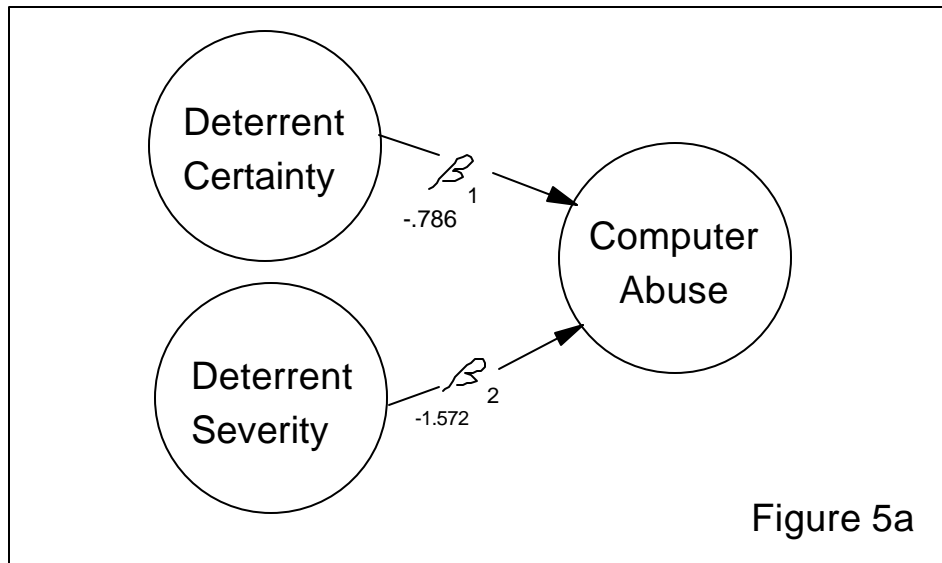


Figure 6. Canonical Correlational Testing of Security Impact Model

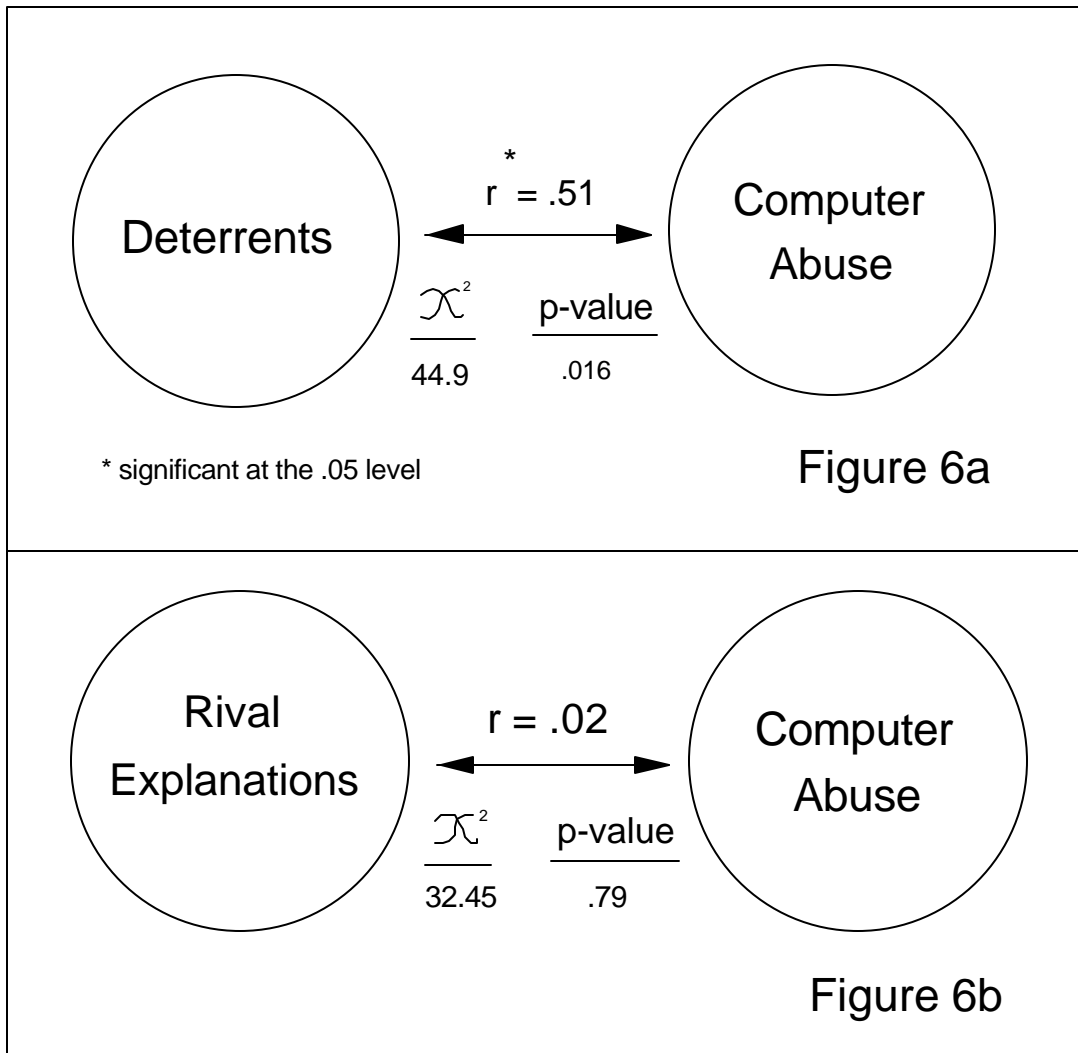


Table 4. Additional Corroborative Testing and Tally of Results

Independent variable	LISREL Test	Canonical Correlational Test	Kruskal-Wallis Test	Chi-Square Test	Total
-----------------------------	--------------------	-------------------------------------	----------------------------	------------------------	--------------

Deterrents

Data Security Hours/Week (Item 14b)	√	√	√ p = .006	√ p = .000	4
Total I/S Security Hours/Week (Item 12)	√	√	√ p = .036	√ p = .004	4
Severity of Disciplinary Actions (Item 19)	√	√	√ p = .016	√ p = .004	4
Number of Informational Sources about System Conduct (Item 18)	√	√	√ p = .000	p = .369	3
Subjective Estimate of Deterrent Effect (Item 22)	√	√	√ p = .000	√ p = .000	4
Number of Full-Time Security Staff (Item 10)	√		p = .055	p = .000	1

Preventives

Number of Security Software Packages in Use (Items 16 and 17)	√		√ p = .000	√ p = .000	3
---	---	--	---------------	---------------	---

Other Motivational-Environmental Factors (Rival Explanations)

Offender Employee/Non-employee Status (Item 31)	√		p = .943	p = .819	1
Motivation of Offender (Item 32)	√		p = .786	p = .732	1
Level of Offender System Privilege (Item 30)	√		p = .639	p = .777	1

References

- ABA (1984). "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.
- AICPA (1984). "Report on the Study of EDP-Related Fraud in the Banking and Insurance Industries," pamphlet, American Institute of Certified Public Accountants, Inc., 1211 Ave. of the Americas, NY, NY.
- Allen, M.J. and W. M. Yen (1979). ***Introduction to Measurement Theory***. Brooks-Cole: Monterey, CA.
- Babbie, Earl R. (1973). ***Survey Research Methods***. Belmont, CA: Wadsworth.
- Bagozzi, Richard P. (1980). ***Causal Methods in Marketing***. New York: John Wiley and Sons.
- Ball, L. and R. Harris (1982). "SMIS Member: A Membership Analysis," ***MIS Quarterly***, Vol. 6, No. 1 (March), 19-38.
- Bielby, William T. and Robert M. Hauser (1977). "Structural Equation Models" in ***Annual Review of Sociology***, Vol. 3, pp. 137-161.
- BloomBecker, Jay (1986). ***Computer Crime, Computer Abuse, Computer Ethics***. Los Angeles, CA: National Center for Computer Crime Data.
- Blumstein, Alfred, Jacqueline Cohen, and Daniel Nagin (1978). "Introduction" in ***Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates***. Washington, D.C.: National Academy of Sciences.
- Brancheau, James and James C. Wetherbe (1987). "Key Issues in Information Systems--1986," ***MIS Quarterly***, Vol. 11, No. 1 (March), 23-45.
- Buikhuisen, W. (1974). "General Deterrence: Research and Theory," ***Abstracts on Criminology and Penology***, Vol. 14, No. 3, 285-288.

- Campbell, Donald (1960). "Recommendations for APA Test Standards Regarding Construct, Trait, and Discriminant Validity," **American Psychologist**, Vol. 15 (August), 546-553.
- Campbell, Donald T. and Donald W. Fiske (1959). "Convergent and Discriminant Validation by the Multitrait-Multimethod Matrix," **Psychological Bulletin**, Vol. 56 (March), 81-105.
- Chambliss, R. (1967). "Types of Deviance and the Effectiveness of Legal Sanctions," **Wisconsin Law Review**, 708.
- Cook, Philip J. (1982). "Research in Criminal Deterrence: Laying the Groundwork for the Second Decade" in **Crime and Justice: An Annual Review of Research**, edited by N. Morris and M. Tonry, Vol. 2. Chicago: the University of Chicago Press., 211-268.
- Cook, Thomas D. and Donald T. Campbell (1979). **Quasi-Experimentation: Design and Analytical Issues for Field Settings**. Chicago: Rand McNally.
- Cronbach, Lee J. (1971). "Test Validation" in **Educational Measurement**, 2nd. Edition, ed. R.L. Thorndike, Washington, D.C.: American Council on Education, pp. 443-507.
- Dickson, G. W., R. L. Leitheiser, J. C. Wetherbe, and M. Nechis (1984). "Key Information Systems Issues for the 80's," **MIS Quarterly**, Vol. 8, No. 3 (September), 135-159.
- Dubin, Robert (1978). **Theory Building** Revised Edition. New York: The Free Press.
- Dunn, Thurman Stanley (1982). "Methodology for the Optimization of Resources in the Detection of Computer Fraud," doctoral dissertation, University of Arizona.
- Ehrlich, L. (1973). "Participation in Illegitimate Activities: A Theoretical and Empirical Investigation," **Journal of Political Economy**, Vol. 81, 521-564.
- Ernst and Whinney (1990). "Ernst & Whinney 1989 Computer Security Survey Report," pamphlet, Ernst & Young, 1400 Pillsbury Center, Minneapolis, MN 55402

- Friedman, Michael (1988). "Access-control Software," **Information Age**, Vol. 10, No. 3 (July), 157-161.
- Goodhue, Dale L. and Detmar W. Straub (1988). "Security Concerns of System Users: A Proposed Study of User Perceptions of the Adequacy of Security Measures," **Proceedings of the 22nd Annual Hawaii International Conference on System Science (HICSS)**, Kona, HA, January.
- Greenberg, David F. and Ronald C. Kessler (1982). "Model Specification in Dynamic Analyses of Crime Deterrence" in **Deterrence Reconsidered: Methodological Innovations**, ed. John Hagan. Beverly Hills, CA: Sage.
- Hair, Joseph F., Jr., Rolph E. Anderson, Ronald L. Tatham, and Bernie J. Grabowsky (1979). **Multivariate Data Analysis**. Tulsa: PPC Books.
- Hartlog, Curt and Martin Herbert (1986). "1985 Opinion Survey of MIS Managers: Key Issues," **MIS Quarterly**, Vol. 10, No. 4 (December), 351-361.
- Hoffer, Jeffrey A. and Detmar W. Straub (1989). "The 9 to 5 Underground: Are You Policing Computer Crimes?" **Sloan Management Review**, Vol. 30, No. 4 (Summer), 35-44.
- Hsaio, David K., Douglas S. Kerr, and Stuart E. Madnick (1979). **Computer Security**. New York: Academic Press.
- Joreskog, Karl G. and Dag Sorbom (1983). **LISREL: Analysis of Linear Structural Relations by the Method of Maximum Likelihood**. 2nd Edition. Chicago: National Educational Resources.
- Klete, Hans (1975). "Some Minimum Requirements for Legal Sanctioning Systems with Special Emphasis on Detection," in **Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates**, ed. Alfred Blumstein, Jacqueline Cohen, and Daniel Nagin. Washington, D.C.: National Academy of Sciences.
- Kling, Rob (1980). "Computer Abuse and Computer Crime as Organizational Activities," **Computer/Law Journal**, Vol. 2, No. 2, 186-196.

- Kusserow, Richard P. (1983). "Computer-Related Fraud and Abuse in Government Agencies," pamphlet, U.S. Dept. of Health and Human Services, Washington, D.C.
- Lee, John A. N., Gerald Segal, and Rosalie Steier (1986). "Positive Alternatives: A Report on the ACM Panel on Hacking," ***Communications of the ACM***, Vol. 29, No. 4 (April), 297-299.
- Long, J. Scott. (1983). ***Confirmatory Factor Analysis***. Beverly Hills, CA: Sage.
- Madnick, Stuart. (1978). "Management Policies and Procedures Needed for Effective Computer Security," ***Sloan Management Review***, (Fall), 61-74.
- Martin, James (1973). ***Security, Accuracy, and Privacy in Computer Systems***. Englewood Cliffs, NJ: Prentice-Hall.
- Nance, William D. and Detmar W. Straub (1988). "An Investigation into the Use and Usefulness of Security Software in Detecting Computer Abuse," ***Proceedings of the 9th Annual International Conference on Information Systems***, Minneapolis, MN, 283-294.
- Nunnally, Jum C. (1967). ***Psychometric Theory***. New York: McGraw-Hill.
- Parker, Donn B. (1976). ***Crime by Computer***. New York: Scribner's.
- Parker, Donn B. (1981). ***Computer Security Management***. Reston, Va.: Reston.
- Parker, Donn B. (1983). ***Fighting Computer Crime***. New York: Scribner's.
- Paternoster, Raymond, Linda F. Saltzman, Gordon P. Waldo, and Theodore G. Chiricos (1982a). "Causal Ordering in Deterrence Research" in ***Deterrence Reconsidered: Methodological Innovations***. ed. John Hagan. Beverly Hills, CA: Sage.
- Paternoster, Raymond, Linda F. Saltzman, Gordon P. Waldo, and Theodore G. Chiricos (1982b). "Perceived Risk and Deterrence: Methodological Artifacts in Perceptual Deterrence Research," ***Journal of Criminal Law and Criminology***, Vol. 73, No. 3 (Fall), 1238-1258.

- Pearson, Frank S. and Neil Alan Weiner (1985). "Toward and Integration of Criminological Theories," ***Journal of Crime and Criminology***, Vol. 76, No. 1 (Winter), 116-150.
- Richards, Pamela and Charles R. Tittle (1982). "Socioeconomic Status and Perceptions of Personal Arrest Probabilities," ***Criminology***, Vol. 20, No. 3 and 4 (November), 329-346.
- Schwartz, Richard D. and Sonya Orleans (1967). "On Legal Sanctions," ***University of Chicago Law Review***, Vol. 34 (Winter), 274-300.
- Siegel, S. and N.J. Castellan Jr. (1988). ***Nonparametric Statistics for the Social Sciences***. 2nd Edition. New York: McGraw-Hill.
- Silberman, Matthew (1976). "Toward a Theory of Criminal Deterrence," ***American Sociological Review***, Vol. 41 (June), 442-461.
- Skogan, Wesley G. (1981). ***Issues in the Measurement of Victimization***. NCJ-74682. Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics.
- Sokolik, Stanley L. (1980). "Computer Crime--The Need for Deterrent Legislation," ***Computer/Law Journal***, Vol. 2, No. 2 (Spring), 354-382.
- Straub, Detmar W. (1986). "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), 21-31.
- Straub, Detmar W. (1988). "Organizational Structuring of the Computer Security Function," ***Computers & Security***, Vol. 7 (Summer), 1-11.
- Straub, Detmar W. and Jeffrey A. Hoffer (1987). "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 47405) Working Paper #W801.
- Straub, Detmar W. and William D. Nance, (1987). "The Discovery and Prosecution of Computer Abuse: Assessing IS Managerial Responses," IRMIS (Institute for Research on the Management of

Information Systems, Indiana University School of Business,
Bloomington, IN 47405) Working Paper #W708.

Straub, Detmar W. and Cathy Spatz Widom (1984). "Deviancy by Bits and Bytes: Computer Abusers and Control Measures" in ***Computer Security: A Global Challenge***, eds. James H. Finch and E.G. Dougall. Amsterdam: Elsevier Science Publishers B.V. (North-Holland) and IFIP, pp. 91-102.

Taber, John K. (1980). "A Survey of Computer Crime Studies," ***Computer/Law Journal***, Vol. 2, No. 2 (Spring), 275-328.

Tittle, Charles R. (1980). ***Sanctions and Social Deviance: the Question of Deterrence***. NY: Praeger.

Vandaele, Walter (1978). "Participation in Illegitimate Activities: Ehrlich Revisited" in ***Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates***, ed. Alfred Blumstein, Jacqueline Cohen, and Daniel Nagin. Washington, D.C.: National Academy of Sciences.

Wong, Ken. (1985). "Computer Crime - Risk Management and Computer Security," ***Computers & Security***, Vol. 4 (December), 287-295.

APPENDIX

Validated Research Instrument