Security Concerns of System Users: A Proposed Study of User Perceptions of the Adequacy of Security Measures

Dale L. Goodhue Detmar W. Straub*

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

*Authors are listed in alphabetical order.

ABSTRACT

Over the last several years, a number of researchers have raised the issue of the level of security concern among system users, suggesting that security may be undervalued in both centralized and decentralized I/S departments, and among I/S staff as well as end-users. Protective measures often require significant managerial vigilance; an appropriate level of awareness and concern, therefore, may be a prerequisite for adequate security protection.

Based on previous work on individuals' attitudes and beliefs about their information systems environment, a theoretical model of the determinants of security concern is presented. The paper discusses the approach to be used in testing the main assertions of the model using a cross-study comparison of security perceptions from two different survey instruments. The first study, conducted in 1985-86, used a sample base of 1063 randomly-selected DPMA members. The second study surveyed 357 end-users in 10 organizations in the 1986-87 time frame. Data analysis of these research questions will be completed in the near future, but analytical procedures are delineated in the paper.

1.0. Introduction

Over the last several years, a number of researchers have raised the issue of the level of security concern among system users (Carr, 1987; White and Christy, 1987; Benson, 1983). They have suggested that security may be undervalued in both centralized and decentralized I/S departments, and among I/S staff as well as end-users. This lack of security consciousness is believed to be pervasive across all industries and organizational sizes (Dickson, et al., 1985).

This lack of awareness is alarming in the face of mounting empirical evidence that, in fact, security breaches are a significant problem (Straub, 1986c). Since protective measures often require significant managerial vigilance, an appropriate level of awareness and concern may be a prerequisite for adequate security protection. In an environment in which systems are being abused but security consciousness is low, the future health of the organization may be seriously threatened.

Given the importance of security awareness, there is a need for a better understanding of what leads to security concern among users. This paper focuses on the perceptions of system users about the security of their systems. First, how is individual concern related to the actual risk faced? Can individual concern be explained by industry-specific risk factors, and by concrete actions taken in a given company to contain that risk?

Second, is there a profile of system users who are more or less sensitive to security dangers? For example, is the level of concern greater among users who are more computer literate? Does it vary for users of personal data versus those who use departmental or corporate data? Or by degree of managerial versus technical responsibility?

0073-1129/89/0000/0117$01.00 © 1989 IEEE

Based on previous work on individuals' attitudes and beliefs about their information systems environment, a theoretical model is presented which suggests that an individual's belief in the adequacy of security in his organization is a function of 1) the potential for abuse in a given industry, 2) company specific action that has been taken to maintain security, and 3) individual factors such as computer literacy, managerial role, etc. The main assertions of this model will be tested using a cross-study comparison of security perceptions from two different survey instruments. The first study, conducted in 1985-86, used a sample base of 1063 randomly-selected DPMA members. The second study surveyed 357 end-users in 10 organizations in the 1986-87 time frame. Data analysis of these research questions will be completed in the near future, but analytical procedures are delineated here.[1]

2.0. Concern about Security

2.1. Prior Discussions of Security Concern

Little prior empirical work has been done on system user attitudes toward computer security. Bailey and Pearson (1983) did include questions on security of data on their questionnaire measuring user satisfaction. However, when Ives, Olson and Baroudi (1983) refined the Bailey and Pearson instrument, they eliminated the security questions since they did not correlate highly with their measures of overall user satisfaction. Thus, the security questions were removed from the UIS measure because of measurement problems rather than lack of importance--security was rated as moderately important by their respondents.

Security and control have been cited as a key issue in opinion surveys of I/S managers. Since the early 80's, security and control have appeared consistently among the top 20 issues for I/S managers (Ball and Harris, 1982; Martin, 1983; Dickson et al., 1984; Brancheau and Wetherbe, 1987). In Hartlog and Herbert's study (1986), it ranked sixth among I/S managers' key issues, and other authors believe it will be rising in the ratings in years to come (Sprague and McNurlin, 1986).

Although I/S managers have at least marginal concerns about security, non I/S managers seem to be less concerned (Buss and Salerno, 1984). In one study, general managers did not even rank security among the top 20 management issues in the systems domain (Brancheau and Wetherbe, 1987). In spite of the fact that security issues are frequently stressed by both Internal Audit and I/S managers (Mautz, Merten, and Severance, 1984),[2] the value of documentation of systems, backup and recovery procedures, and system access controls are not self-evident. Without a major loss from lax security, it may be the case that security concern will generally be quite low,[3] and top executives will be reluctant to grant status and commit resources to the computer security function (Keefe, 1983).

2.2. Justification for Security Concerns

Should managers be concerned about security, or at least more concerned than they presently are? There is a growing body of evidence that computer systems in many organizations are subject to frequent and persistent abuse. Case histories and sample survey data to date indicate that organizations are reporting a wide range of losses (AICPA, 1984; Colton, 1982a, 1982b; Straub, 1986a; Whiteside, 1978; BloomBecker, 1986). The American Bar Association survey (ABA, 1984) reported total dollar losses of approximately $500 million for 72 firms out of a sample base of 148, with "known and verifiable losses" averaging in the millions of dollars. A large percentage of major firms--25% to 50%--are reportedly uncovering one or more serious incidents of abuse each year (ABA, 1984). Some of these incidents have been catastrophic (Parker, 1984); others, though only minor in actual damage, have been major in their potential for damage (Straub, 1986a). Many other researchers report similarly disturbing figures (Parker, 1976; Wong, 1985; Allen, 1977; Straub, 1986a, and Straub, 1986b).

As computer technology spreads throughout our organizations in the form of End User Computing (EUC), another area of potential risk is emerging. Since EUC is computing in which end users control their inputs, processing stages, and outputs, and even their own software development using fourth generation languages (Rockart and Flannery, 1983), the security risk in this environment is theoretically high. Reports on activities of security administrators and

Information Centers report little or no security training for systems users (Straub, 1986c; Leitheiser and Wetherbe, 1985).

In the case of EUC the threat needs to be taken seriously because EUC is growing at such a phenomenal pace. Rockart and Flannery (1983) predicted that EUC activities in large corporations will grow from 10% of all computing capacity in 1981 to 70% of an expanded capacity in 1990. Leitheiser and Wetherbe (1985) predicted a thirty-fold increase between 1980 and 1990. While organizations have established some central EDP control over their large databases and systems, controls are still rudimentary, if present at all, in EUC.

Thus there are strong reasons to believe that computer abuse is a problem to be reckoned with and one that will not diminish over time of its own accord. Initiatives need to be taken by organizations to contain this significant risk. While managers of I/S and Internal Auditing bear a particular responsibility in this regard, the awareness of all users must be heightened for effective security.

It is appropriate, therefore, that research efforts reveal the circumstances in which low security consciousness is likely to occur. With this knowledge, I/S security administrators, I/S managers, and other managers will be able to exercise greater control over the computing environment. In situations where security consciousness is lower than it should be, the consciousness may be able to be heightened.

3.0. Developing a Model of Perceptions of Security Concern

3.1. User Perceptions as a Theoretical Construct

There are numerous methodological questions about how to clearly measure user perceptions, including user perceptions about security. Although many studies have employed user perceptions as empirical measures (e.g. Zmud, 1978; Ives, Olson, and Baroudi, 1983; Swanson, 1987), there is considerable concern that such measures lack theoretical clarity, in part because they lack a theoretical underpinning (Treacy, 1985; Melone, 1987). The most commonly cited reference discipline for these measures has been job satisfaction research (e.g. Bailey and Pearson, 1983). However, "I/S satisfaction" has not been well enough defined to clarify how it is similar and how different from "job satisfaction" (Goodhue, 1986).

In addition, job satisfaction has been shown to relate only very weakly to performance (Brayfield and Crockett, 1955; Vroom, 1964; Iaffaldano and Muchinsky, 1985). To address these problems, Goodhue (1986) drew upon theory developed in job satisfaction research which distinguished between job "satisfaction" and individual "satisfactoriness" (Dawis, Lofquist and Weiss, 1968). Goodhue (1986) expanded on the original theory to present a model of user attitudes about their systems environment which included perceived "satisfactoriness" of the systems (<u>beliefs</u> about the extent to which the I/S environment that assist the user in performing his or her tasks), and perceived "satisfaction" (<u>feelings</u> about whether the individual's personal needs are satisfied by using systems). Goodhue suggested that user-assessed satisfactoriness should be closely related to performance, and thus was a far better surrogate for I/S success than satisfaction.

According to this theory, a user's assessment of the satisfactoriness of his systems environment depends upon three interacting constructs: the user's task characteristics (and thus his demands upon the I/S environment), the characteristics of the I/S environment itself, and individual characteristics. Thus, Goodhue suggested that a person whose job related tasks were fairly straight-forward and did not require much from the systems environment, would probably find the systems environment satisfactory, regardless of its characteristics.

3.2. Satisfactoriness Applied to the Realm of Security Concern

If we apply the theory of satisfactoriness to the perceptions of data security, the concepts of task, I/S environment, and individual characteristics must be placed in the domain of providing data security in an organization. In order to do this the task users face must first be defined.

In the case of security the task is protecting the data of the organization from intentional or unintentional misuse. The ideal person to ask this question of is someone charged with, or intimately aware of the degree to which data is being safeguarded. As we move to users who are less concerned with security as part of their jobs, we can expect the security concept to be less salient, users to be less informed, and measures of security concern to contain more error.

The difficulty of the task of protecting data from intentional misuse should vary as the potential for gain on the part of the abuser, or loss on the part of the company, varies. For example, in the information-intensive financial industry there would be more potential for gain from unscrupulous persons manipulating data for their own advantage, than, for example, in the manufacturing industry. Thus the difficulty of achieving satisfactory security should be greater in the financial industry. (Though the potential for industrial espionage might be greater in some manufacturing environments, the risk in the finance industry might be expected to be higher.) Thus all things being equal, we would expect persons in industries with a high degree of security danger to be more concerned about security, and to feel that their environment is less satisfactory.

The second major factor contributing to perceptions of the satisfactoriness of the security environment is action taken by corporations to prevent security violations. It would be expected that in firms which devote many person-hours and considerable software to protecting data from misuse, individuals would be less concerned, and feel that the security was more satisfactory. Thus all other things being equal, we would expect that persons in firms which devoted more resources to providing security would be less concerned about security, and to feel that their environment is more satisfactory.

Finally there are individual factors. Awareness of the potential problem is a major consideration here. We might expect that persons who are more aware of the potential for abuse would be sensitized to the dangers of inadequate security, and would be more likely to feel that security was unsatisfactory. Thus all other things being equal, we would expect that greater awareness of potential abuse would lead to more concern about security, and perceptions that the environment was more unsatisfactory. To be more specific, we might expect that persons who were more computer literate would be more aware of the potential for abuse, DP personnel more aware than non-DP users, and data accessors and data analysts more aware than decision makers with low personal contact with the technology of data storage.

Figure 1 shows our model of the determinants of security concern. It suggests the following propositions about the relationship between user assessment of the satisfactoriness of security measures and the three contributing factors:

Proposition 1. As the risk to the organization increases (i.e. potential gain for the perpetrator, and/or potential damage for the organization), perceptions of the satisfactoriness of security measures will decrease, ceteris paribus.

Proposition 2. As the resources applied to maintain security increase, perceptions of the satisfactoriness of security measures will increase, ceteris paribus.

Proposition 3. Users who are more aware of the potential of computer abuse (i.e. they are more computer literate, and/or more closely associated with the use of the computer technology), will have lower levels of perceived satisfactoriness of security measures, ceteris paribus.

Proposition 4. There should be an interaction between user awareness and sensitivity to risk and company action. That is, perceptions of users who are more aware of the dangers should be more affected by differences in risk and company action than those who are unaware of the dangers.

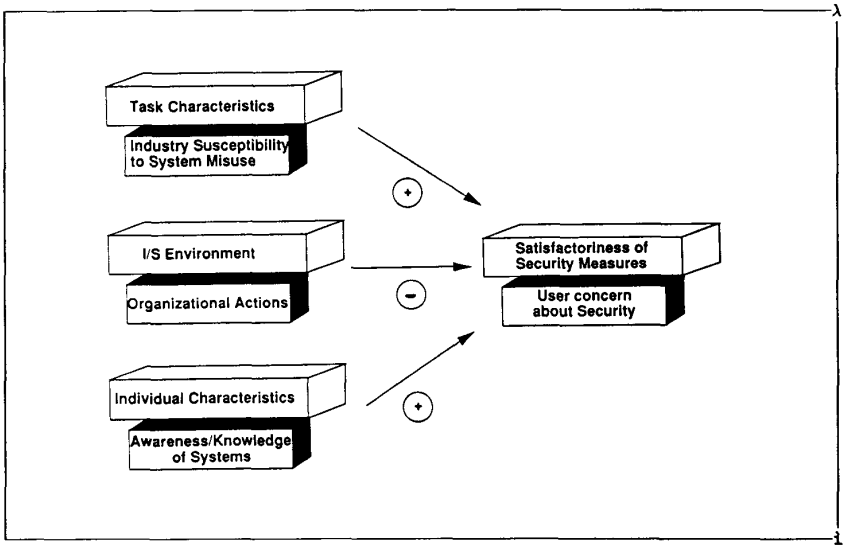

Figure 1. Theoretical Model of Security Concern

4.0. Methodology for Testing the Model

These four propositions will be tested using data from two different data collection efforts. The first sample, conducted in 1985-86, used a base of 1063 randomly-selected DPMA members. This sample included measures of all the key concepts in the propositions, and can be used to test all four propositions. The second sample surveyed 357 end-users in 10 organizations in the 1986-87 time frame. This sample has more extensive coverage of individual characteristics, but no coverage of the resources applied to security measures. Thus only proposition 3 can be tested with this data.

4.1. Study #1

Data for this study was drawn from a victimization database obtained in a prior study of computer abuse and deterrent countermeasures (Straub, 1986c). The survey instrument was validated via extensive field interviews with 35 system professionals, interviews and questionnaire responses from an independent group of 88, and, finally, pilot study questionnaire returns from 170 respondents. The validated survey was mailed out to randomly-selected DPMA (Data Processing Management Association) members in 1986. The sample base that resulted from this study and the pilot group, with duplicates removed, was 1063. The validation process and tests for non response bias are discussed at length in Straub (1986c).

In this sample, the bulk of respondents were systems professionals, ranging from CIOs to programmer-analysts. There were also a significant number of computer security specialists in the sample. The sample, in short, may be characterized as a sample of I/S professionals.

4.1.1. Measures

The concern a system user experiences about security is predicted to be a function of three different constructs--industry risk, company actions, and individual awareness. The measures used for each of these constructs are shown in Table 1.

Concepts	Research Construct	Measure Description
Satisfact-oriness of Security Measures	User Concern about Security	-Subjective evaluation of security effectiveness (rated on a 0 to 7 scale)
Task Char-acteristics	Industry Sus-ceptibility to System Misuse	-Industry type (12 dummy vars) -Manuf. and Processing -Chemical or Pharmaceutical -Govt. Fed or Local incl Mil. -Educational -Computer and DP Services -Financial: banks, insur. etc -Wholesale or Retail Trade -Medical and Legal Services -Petroleum -Transportation Services -Utilities -Construction, Mining, Agri.
I/S Envir-onment	Organizational Actions	-Total personnel hours/week devoted to security functions
Individual Character-istics	Awareness/ Knowledge of Systems	-Years experience in Info sys. -Managerial level and user/systems staff status

Table 1. Concepts, Constructs, and Measures For Sample #1[4]

To measure the independent and dependent variables, the survey used an anonymous questionnaire that asked respondents for general information about themselves and their organizations and more pointed questions about their security operations and the times they have been victimized. The questionnaire evolved from a draft instrument and pre-testing interviews with 35 systems professionals. A revised instrument was then validated via a pilot survey of 1000 randomly-selected DPMA members and multi-trait, multi-method analysis (MTMM), an intricate interview-questionnaire comparison technique (Straub, 1986b). In the latter, 44 interviews with system professionals working in industries of all sizes and types were compared with responses from questionnaires filled out by 44 others, matched on organization (Straub, 1986b). Validation is vital in producing a questionnaire that is clear and unambiguous. At the same time, it ensures that the data collected will answer key research questions.

4.1.2. Testing of the Predicted Relationships

The procedure to be used is to first test a main effects model, and then to determine empirically whether adding the hypothesized interaction effects improves the model fit to the data. The main effects model (with no interaction effects) will be tested by regressing the dependent variable, concern about security, against the predicted independent variables (industry risk, organization actions and individual characteristics).

In testing for interaction effects, the main effects regression model (from above) will be used as the baseline model, and interaction effects will be added to the baseline one at a time. For each interaction effect tested, the new adjusted R-Squared statistic can be noted. If the adjusted R-Squared decreases, the interaction effect is not empirically supported. If the adjusted R-Squared statistic increases, an F test can be performed on the two regressions to

determine the likelihood that the interaction effect is a predictor of security concern.

4.2. Study #2

Data for this sample was drawn from 357 questionnaires administered in 10 organizations during 1986-87 as part of a study of user assessments of the satisfactoriness of their I/S environments. The companies may have been self selected based on their interest in end user computing, and thus may represent a bias toward forward-thinking companies, or companies where EUC is appropriate.

In each of the 10 companies, at least two groups of users were targeted, and for each group about 20 users were selected on as random a basis as practical considerations would allow. All of the respondents were non I/S "users" of computer data in some form, but there was no effort to identify users who were conscious of or involved in data security issues. Since the bulk of the respondents in this sample were end users of computer systems, rather than systems professionals, this sample can be characterized as a sample of End-Users.

The response rate in each company varied from about 50% to 100%, with an overall response rate of 75%. Five percent of the total were unusable because of incomplete or unconscientious data (for example, answering all questions with "neither agree nor disagree"). When these were removed, there remained 357 usable questionnaires, or about 70% of the number sent out.

4.2.2. Measures

Measures from the questionnaire, summarized in Table 2, "Concepts, Constructs, and Measures For Study #2," were designed to gauge the level of concern system users felt about their security, and to gather data about independent variables that presumably correlate highly with, and affect the level of concern. Because there were three separate questions measuring the level of concern with security, we can determine that this construct has been measured with high reliability. These three questions were randomly placed in a list of over 50 questions about all aspects of the I/S environment and were more highly correlated with each other than with any other questions in this analysis, which is evidence of their discriminant validity and their reliability. Cronbach's alpha for these variables was .84.

For the other constructs within the individual characteristics concept, there were only single questions, or several related but not redundant questions. For example, respondents were asked to indicate the relative percentages of their tasks which would be characterized as decision-making, as analysis, and as accessing data. The 16 individual characteristics questions will be factor analyzed to identify the major underlying dimensions. However, because the underlying dimensions have not been hypothesized in advance, both the underlying dimensions and their measures must be viewed as exploratory rather than validated.

4.2.3. Testing of the Predicted Relationships

The concern a system user experiences about security is predicted to be a function of three sets of variables--industry susceptibility, company actions, and individual awareness. Since Study #2 included no measures for company actions, our ability to test the theoretical model is limited. A portion of the model can be tested, however, by making the assumption that both the industry susceptibility and the company actions are constant within any given company. By subtracting the company mean from the concern score of every respondent, we can determine the "residual concern" which is presumed to be a function of individual characteristics.

Given a measure of residual concern, it will be possible to test the relationship between this derived variable and the measured individual characteristics. This will be done by regressing "residual concern" as a function of the underlying dimensions of individual characteristics.

Concepts	Research Construct	Measure Description	Number of Questions
Satisfact-oriness of Security Measures	User Concern about Security	-User assessment of security effectiveness	3
Individual Character-istics	Awareness/ Knowledge of Systems	-Computer literacy measure	1
		-Source of data used by respondent (reports, terminal access to central hardware, or Standalone PC's)	3
		-degree to which respondent is engaged in decision making vs. analysis or data access	8
		-degree to which respondent uses personal, department, corporate, or external data	4

Table 2. Concepts, Constructs, and Measures For Sample #2

5.0. Discussion

In this paper we have argued that insufficient computer and data security is a major problem in many organizations, and that low levels of concern contribute to the danger. In particular, without appropriate levels of managerial concern, many actions to bolster security may be much less effective. It is important, therefore, to understand the causal factors that contribute to higher levels of security concern, so that management can address inappropriately low levels where they exist.

Drawing on previous work on user attitudes about their systems environment, we have proposed a model of the determinants of users' perceptions of the adequacy of the security of their systems and data. Several propositions were suggested as tests of the model. Finally, the methodology to be used in empirically testing these propositions with two independent studies was discussed.

Preliminary analysis suggests that several of the assertions of the model are supported by statistically significant relationships, but that the total explanatory power of the model is low. This suggests that there may be refinements to the theoretical model which would improve its explanatory power; it also suggests that security concern will need to be very carefully measured in future research.

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.

Alavi, Maryam, and Ira R. Weiss (1985). "Managing the Risks Associated with End User Computing," Journal of Management Information Systems, Vol. 2, No. 3 (Winter), 5 - 20.

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

Bailey, J.E. and Pearson, S.W. "Development of a Tool Measuring and Analyzing Computer User Satisfaction," Management Science, Vol. 29, No. 5, May 1983, pp. 530-544.

Ball, L. and R. Harris (1982). "SMIS Member: A Membership Analysis," MIS Quarterly, Vol. 6, No. 1 (March), 19-38.

Benson, David H. (1983). "A Field Study of End User Computing: Findings and Issues," MIS Quarterly, Vol. 7, No. 4, 35-45.

Bezdek, Jiri (1984). "Across-the-Board Training Protects Data: Crime Requires Preventive Action by Execs," Computerworld, 29 October, 1984, 10-11.

BloomBecker, Jay (1986). Computer Crime, Computer Security, Computer Ethics. Los Angeles, CA: National Center for Computer Crime Data.

Brancheau, James and James C. Wetherbe (1987). "Key Issues in Information Systems--1986," MIS Quarterly, Vol. 11, No. 1 (March), 23-45.

Brayfield, A.H. and Crockett, W.H. (1955). "Employee Attitudes and Employee Performance," Psychological Bulletin, Vol. 52, No. 5, 396-424.

Brickman, Bruce K. (1983). "The Corporate Computer: A Potential Timebomb," Financial Executive, Vol. 51, No. 4 (April), pp. 20, 22, 24.

Buss, Martin D.J. and Lynn M. Salerno (1984). "Common Sense and Computer Security," Harvard Business Review, Vol. 62, No. 2 (March-April), 112-121.

Carr, H. H. (1987). "Information Centers: The IBM Model Vs. Practice," MIS Quarterly, Vol. 11, No. 3. (September), 324-338.

Colton, Kent W., et al. (1982a). "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. Referenced by special permission.

Colton, Kent W., et al. (1982b). Computer Crime: Electronic Fund Transfer Systems and Crime. Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics.

Dawis, R.V., L.H. Lofquist, and D.J. Weiss (1968). A Theory of Work Adjustment: A Revision. Minnesota Studies in Vocational Rehabilitation: XXIII, Industrial Relations Center, Bulletin 47, University of Minnesota, Minneapolis, MN.

Dickson, G. W., G. B. Davis, and T. R. Hoffman (1985). "A Forecast of Future Information Technology and Its Managerial and Educational Implications," Conference for the Administrative Sciences Association of Canada (ASAC), Montreal, May 1985.

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.

Fisher, Royal P. (1984). Information Systems Security. Englewood Cliffs, NJ: Prentice-Hall.

Goodhue, Dale L. (1986). "IS Attitudes toward Theoretical and Definitional Clarity," Proceedings of the Seventh International Conference on Information Systems, San Diego, CA, pp. 181-194.

Hartlog, Curt and Martin Herbert (1986). "1985 Opinion Survey of MIS Managers: Key Issues," MIS Quarterly, Vol. 10, No. 4 (December), 351-361.

Hollinger, Richard C. and Lonn Lanza-Kaduce (1988). "The Process of Criminalization: the Case of Computer Crime Laws," Criminology, Vol. 26, No. 1 (February), 101-126.

Iaffaldano, M.T. and Muchinsky, P.M. "Job Satisfaction and Job Performance: A Meta-Analysis," Psychological Bulletin, Vol. 97, No. 2, pp. 251-273.

Ives, B., Olson, M.H., and Baroudi, J.J. (1983). "The Measurement of User Information Satisfaction," Communications of the ACM, Vol. 26, No. 10 (October), 785-793.

Katz, David M. (1984). "Keeping Up with Computer Capers," National Underwriter, 24 February, 1984, pp. 2, 18-19.

Keefe, Patricia (1983). "Computer Crime Insurance Available--For a Price," Computerworld, 31 October, 1983, 20-21.

Leitheiser, and J.C. Wetherbe (1985). "Service Support Levels: An Organized Approach to End-User Computing," MIS Quarterly, Vol. 10, No. 4 (December), 337-350.

Martin, E.W. (1983). "Information Needs of Top MIS Managers," MIS Quarterly, Vol. 7, No. 1 (September), 1-11.

Mautz, Robert K., Alan G. Merten, and Dennis G. Severance (1984). "Corporate Computer Control Guide," Financial Executive, Vol. 52, No. 6 (June), 25-36.

Melone, N. P. (1988). "Suggestions For a Theory-Based Alternative to the "User-Satisfaction" Construct in Information-System Research" GSIA Working Paper No. 13-87-88, Graduate School of Industrial Administration, Pittsburgh, PA, Revised October, 1987.

Parker, Donn B. (1976). Crime by Computer. New York: Scribner's.

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

Shoor, Rita (1986). "Microcomputer Security: Back to Basics," Infosystems, Vol. 33, No. 9 (September), 44-46.

Sprague, Ralph H., Jr. and Barbara C. McNurlin, eds. (1986). Information Systems Management in Practice. Englewood Cliffs, NJ: Prentice-Hall.

Straub, Detmar W. (1986a). "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. (1986b). "Instrument Validation in the MIS Research Process," Proceedings of the Annual ASAC (Administrative Sciences Association of Canada) Conference, June 1-3, Whistler, B.C.

Straub, Detmar W. (1986c). "Deterring Computer Abuse: the Effectiveness of Deterrent Countermeasures in the Computer Security Environment," doctoral dissertation, Indiana University School of Business, Bloomington, IN.

Swanson, E.B. "Information Channel Disposition and Use," Decision Sciences, Vol. 18, No. 1, 1987, pp. 131-145.

Treacy, M.E. "An Empirical Examination of a Causal Model of User Information Satisfaction," unpublished working paper, Center for Information Systems Research, Sloan School of Management, MIT, April, 1985.

Vroom, V.H. Work And Motivation, John Wiley & Sons, New York, 1964.

White, C. E. and D. P. Christy (1987). "The Information Concept: A Normative Model and a Study of Six Installations," MIS Quarterly, Vol. 11, No. 4, (December), pp. 450-458.

Whiteside, Thomas. (1978). Computer Capers. New York: New American Library.

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

Zmud, R.W. (1978). "An Empirical Investigation of the Dimensionality of the Concept of Information," Decision Sciences, Vol. 9, No. 2, 187-195.

Endnotes

1. Portions of this work were carried out under the auspices of International DPMA (Data Processing Management Association). It was supported by grants from CISR (Center for Information Systems Research, Sloan School of Management, Massachusetts Institute of Technology), IBM, IRMIS (Institute for Research on the Management of Information Systems, Indiana University Graduate School of Business), the Ball Corporation Foundation, and the MIS Research Center (University of Minnesota, Carlson School of Management).

2. Shoor (1986) feels that executives are aware of the security problem and are willing to help prevent it. The evidence would tend to refute this view, however.

3. Major losses from computer abuse, in fact, are a primary causal factor for the initiation of security administration (Straub, 1986).

4. Coding of managerial status was based on the position title checked off in Item 1. Vice Presidents and CEOs were coded as top managers. EDP Directors were coded as middle level managers as were Directors of EDP Auditing and Plant Security. Positions normally reporting to middle managers were coded as line managers. Also, any position that was not clearly in the systems area was coded as "User."