December 2001

Value-Focused Assessment of Information System Security in Organizations

Gurpreet Dhillon
University of Nevada, Las Vegas

Gholamreza Torkzadeh
University of Nevada, Las Vegas

VALUE-FOCUSED ASSESSMENT OF INFORMATION SYSTEM SECURITY IN ORGANIZATIONS

Gurpreet Dhillon
College of Business
University of Nevada, Las Vegas
dhillon@ccmail.nevada.edu

Gholamreza Torkzadeh
College of Business
University of Nevada, Las Vegas
torkz@ccmail.nevada.edu

Abstract

This paper presents findings of an empirical study of information system (IS) security values adhered to by user managers in a cross section of firms in various industries. Using Keeney's (1999) value-focused thinking *approach, 73 managers were interviewed to identify a set of fundamental and means values that are essential in protecting the information resources of a firm. The findings are used to develop a theoretical framework for conceptualizing individual and organizational issues in managing IS security. The proposed framework will be an appropriate underpinning for the development of an instrument for measuring IS security concerns.*

Keywords: IS security, security values, value-focused thinking.

UNDERTAKING A VALUE-FOCUSED ASSESSMENT OF IS SECURITY

IS security as an issue is increasingly gaining importance in managing the information resources of a firm. Not only has there been an increase in the number of cited IS security breaches, but the annual spending on security measures is expected to grow from $8.7 billion in 2000 to $30.3 billion in 2005—28% growth year by year (as reported in *CIO Magazine*, July 15, 1999). Over the years, a number of security approaches have been developed that help in managing IS security and in limiting chances of an IS security breach. The various approaches fall into three broad categories: checklists, risk analysis, and evaluation methods.

Checklists, as a means to manage IS security, have gained significant popularity over the past two decades (e.g., SAFE and AFIPS checklists). However, checklists have come under criticism since exclusive attention is given to the observable events rather than the social nature of the problem (Backhouse and Dhillon 1996) and "what can be done" rather than "what needs to be done" (Baskerville 1993).

The use of risk analysis as a means to ensure protection has perhaps been the most influential technique in dealing with IS security of commercial enterprises. A number of tools have been developed to support the practice of risk analysis (e.g., CRAMM, MARION, and RISKPAC). Most IS security risk management approaches attempt to identify the level of risk based on the product of probability of occurrence of adverse events and the estimated cost associated with the loss (see the methodologies proposed by Courtney 1977; Krueger 1993; Loch et al. 1992). Although IS security risk analysis approaches help in generating a risk profile of context specific threats that have occurred in the past, they fall short of interpreting risks for novel IS implementations (see the arguments proposed by Straub and Welke 1998; Willcocks and Margetts 1994).

The third category of IS security approaches have their roots in the evaluation methods, used extensively by the U.S. Department of Defense. The evaluation methods tend to analyze the level of compliance of pieces of software to predetermined security standards. A number of evaluation methods have been in existence for the past three decades (e.g., TCSEC, ITSEC, BS7799). Over the years, although the evaluation criteria have worked adequately for the U.S. Department of Defense, they seem to have their limitations in their application to commercial environments. This is essentially because they were developed for a very well defined environment, i.e., the military organization, and business organizations represent a different reality, hence questioning the validity and completeness of the underlying models (Dhillon 2001).

Since annual security related losses have been on the increase, current means for managing IS security have been unable to fulfill the promise. As Dhillon and Backhouse (2001) point out, most IS security approaches tend to offer narrow, technically oriented solutions, whereas managing IS security needs to adopt a socio-organizational perspective (as suggested by Baskerville 1993; Dhillon and Backhouse 2001; Straub and Welke 1998). Such a perspective can be adopted by conducting a value-focused assessment of IS security in organizations.

There are two classes of definitions that need to be considered when conducting a value-focused assessment of IS security. The first relates to the notion of value-focused assessment itself. Values, according to Keeney (1999), are principles for evaluating the desirability of any possible consequence and are hence essential to assess the "actual or potential consequences of action and inaction" in a given decision context (Keeney 1992, pg. 6). With respect to IS security management, our decision context is to maximize IS security so as to protect the information resources of the firm. Although there can be no value proposition for IS security *per se* since IS security is not a product or service, we can think of value propositions to an individual in an organization as well as the various groups and divisions in a firm. Hence the value proposition associated with IS security is defined as the net benefit and cost associated with maintaining the security and integrity of the computer-based IS and the organization. The second class of definitions relates to IS security. IS security is defined as minimizing the risks arising because of inconsistent and incoherent behavior with respect to information handling activities in an organization. It is important to consider IS security in this light since security is not just a technical problem. As Strens and Dobson (1993) note, it is a social and organizational problem because technical systems have to be operated and used by people.

This paper is organized into three sections. Following this brief introduction, which systematically positions the nature and scope of this research, section two presents the results and methodology used to collect the values attached to IS security. The third section presents the conclusions and a discussion of our future research emphasis.

METHODOLOGY

Methodologically, this study is based on the concept of value-focused thinking as proposed by Keeney (1999). Keeney (1992) suggests that value-focused thinking is more useful than the usual "alternative-focused thinking" since no limits are enforced in identifying "what we care about." According to Keeney, alternatives are a means to achieve the more fundamental values, while values inform the relative desirability of consequences. Hence by identifying values one is able to decide what one wants and then figure out how to get it (see Keeney 1992, pg. 5). Research conducted by Keeney (1994, 1999) has exposed underlying values in a wide array of contexts. Keeney's inherent argument has been that the value-thinking process helps researchers and managers alike to be proactive in creating more value options instead of being limited to available alternatives.

The value thinking process involves three steps. First, interviews are conducted to elicit values that individuals might have within the decision context. The output of the interviews would generally result in a long list of individual wishes. Second, the individual values and statements are converted into a common format. This is generally in the form of an objective (i.e., object and a preference). Third, the objectives are classified as either being fundamental with respect to the decision context or merely a means to support or inform fundamental objectives. The means and fundamental objectives are then organized into a network. In the context of our research, the three step process is applied to assess the values attached by user managers to protect the information resources of a firm (i.e., provide security). In all, 73 user managers were interviewed from a broad range of businesses in the southwestern United States. Businesses represented the following industries: banking, IT, telecommunications, hotel, management consulting, manufacturing, pharmaceuticals, and health care.

Identifying values. Keeney recommends that the best possible way to identify values is to ask the concerned people. In order to elicit the values, a number of techniques are suggested. These include the creation of a wish list, posing alternatives, identifying problems and shortcomings, to name a few. Since individuals may express various values differently, there is an inherent difficulty with the latency of the values. In order to overcome this problem, multiple probing techniques were used to identify the latent values. Such probes were prepared beforehand and included questions such as: "If you did not have any constraints, what would your objectives be?" "What needs to be changed from the status quo?" "How do you evaluate whether IS security is being maintained?" "How do you tell if IS security is being compromised?" On an average, we spent 40 minutes with each individual trying to elicit what mattered most in protecting the information resources of the firm. Our goal was to understand all possible factors that influenced individual and group behavior toward IS security and what values they had with respect to managing IS security. The 73 interviews with user managers resulted in 411 wishes/problems/concerns/values.

Structuring objectives. The second step in assessing values is to structure the objectives. The output of step one, the initial list of values, has multiple forms: importance of trust, privacy problems, confidentiality, minimizing disregard for laws. Since it is useful to develop consistency in the expressions, each of the values was converted into a corresponding objective. According to Keeney (1999), an objective is constituted of the decision context, an object, and a direction of preferences. In the case of this study, the decision context is adequate management of IS security and values such as "personal integrity of employees is important" becomes "maximize employee integrity," "security is an issue of confidentiality" becomes "emphasize importance of confidentiality," and so forth. A total of 93 objectives were developed from the initial list of values. The 93 objectives were further clustered into 25 groups since multiple objectives tend to address a particular issue. For example, "creating user passwords," "provide several levels of user access," and "control accessibility to information" are all objectives that help in "maximizing access control."

Organizing objectives. The initial list of objectives generated in the second step includes both the means and fundamental objectives. It is important to differentiate the two by repeatedly linking objectives through means-ends relationships and specifying fundamental objectives. In identifying the fundamental objectives, it is important to ask, "Why is this objective important in the decision context?" (Keeney 1999, pg. 66). In our study, if the answer was that the objective is one of the essential reasons for interest in adequately managing IS security the objective was a candidate for a fundamental objective. However, if the objective was important because of its implications for some other objective, it was a candidate for a means objective. For example, "promoting individual work ethic" is one of the fundamental objectives for maximizing IS security, but "instilling personal morals" is a means to achieve personal integrity and hence is designated as a means objective. By systematically following this process, a total of nine fundamental and 16 means objectives were identified. These are presented in Tables 1 and 2 respectively. The means and ends objectives network, developed using directional relationships, is presented in Figure 1. For parsimony, these tables provide an example of items for each factor. However, a complete list of items is available from the authors.

Table 1. Means Objectives Related to IS Security

Improve authority structures Example: Clarify delegation of authority	**Maximize fulfillment of personal needs** Example: Appreciate personal needs for job enhancement
Increase communication Example: Minimize curiosity by open communication	**Enhance understanding of personal financial situation** Example: Understand the needs of different level of financial status
Promote responsibility and accountability Example: Clarify delegation of responsibilities	**Understand individual characteristics** Example: Understand demographics with potential to subvert controls
Establish ownership information Example: Emphasize importance of confidentiality	**Ensure legal and procedural compliance** Example: Minimize the disregard for laws
Increase trust Example: Display employer trust in employees	**Understand personal beliefs** Example: Understand effect of religious beliefs on security
Understand work situation Example: Minimize need to have leverage on others	**Maximize availability of information** Example: Ensure adequate procedures for availability of information
Optimize work allocation practices Example: Distribute workload evenly	Ensure censure Example: Instill a fear of consequences
Maximize access control Example: Create user passwords	
Ensure empowerment Example: Promote empowerment in the organization	

Table 2. Fundamental Objectives Related to IS Security

Overall Objective: Maximize IS Security	
Maximize awareness Example: Create an environment that promotes awareness	**Maximize data integrity** Example: Minimize unauthorized changes
Adequate human resource management practices Example: Provide necessary job resources	**Maximize organizational integrity** Example: Create an environment of managerial support
Developing and sustaining an ethical environment Example: Develop an understood value system in the organization	**Maximize privacy** Example: Emphasize importance of privacy
Enhance integrity of business processes Example: Develop understanding of procedures	**Promote individual work ethics** Example: Minimize temptation to steal information
Enhanced management development practices Example: Maximize individual comfort level of computers/software	

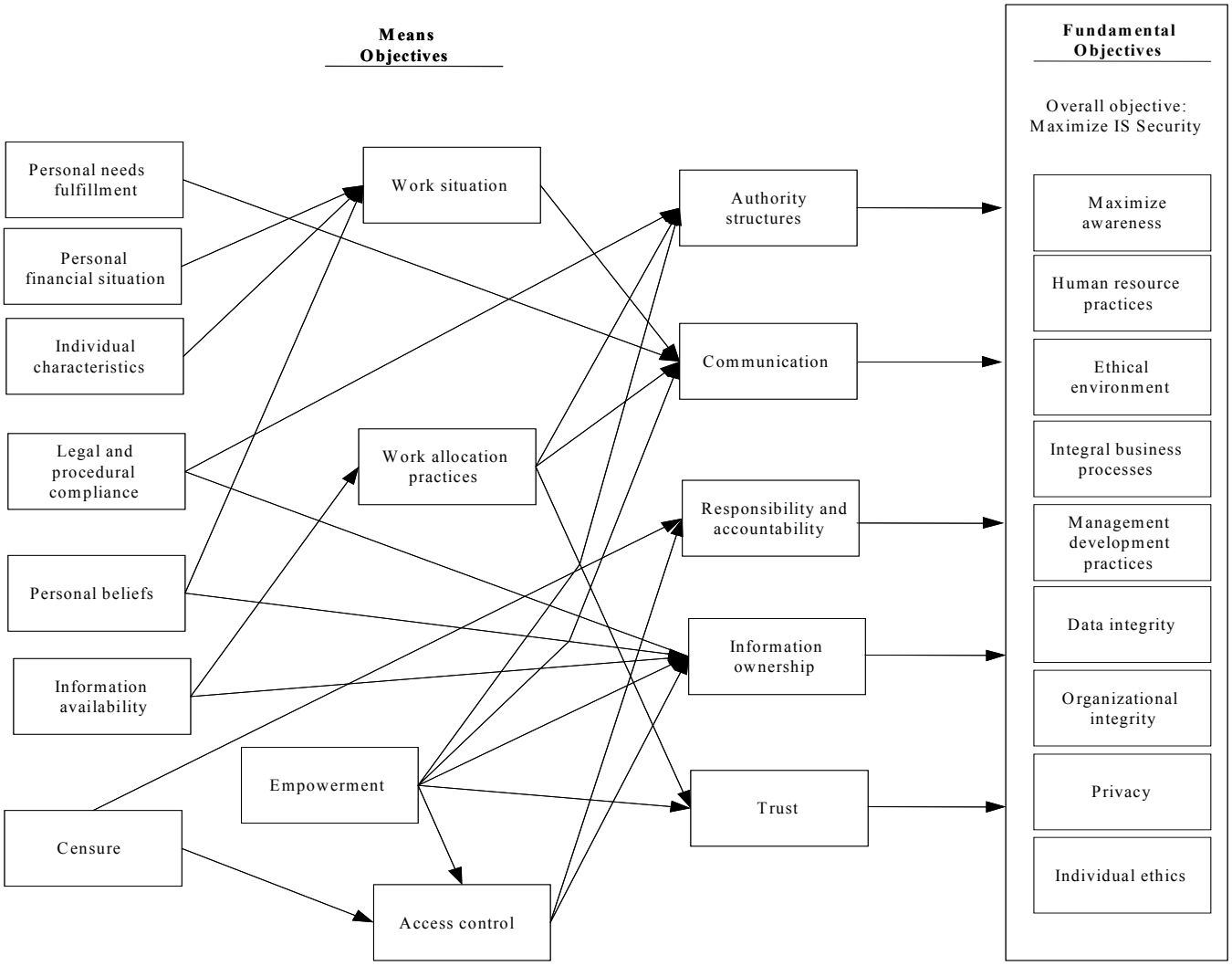

Figure 1. A Means-Ends Objectives Network for IS Security

CONCLUSION AND FOLLOW-UP STUDY

This study follows a value-based approach to identify a broad set of factors that may be instrumental in shaping a favorable security outcome in various organizations. In order to ensure generalizability of the findings of this study, we solicited responses from active user managers of information technologies in diverse industries. These respondents were asked to consider broad issues and concerns that they perceived as relevant to IS security in their organization. Responses were carefully analyzed and results grouped and presented in terms of means objectives and fundamental objectives which, when combined, will provide an appropriate base for the development of success measures for IS security. A network of relationships is presented that suggests how means objectives may interact and influence fundamental objectives and ultimately the overall objective of maximizing IS security.

We are encouraged by the findings of this study and intend to proceed with the follow-up study. The specific goals of the follow-up study are to (1) continue an in-depth case study (currently in progress) that will further strengthen the validity of each factor, (2) develop a final definition for each construct, and (3) generate measures representing these factors, gather data for psychometric analysis of measures, and recommend a measurement for IS security success that is reliable and valid.

References

Backhouse, J., and Dhillon, G. "Structures of Responsibility and Security of Information Systems," *European Journal of Information Systems* (5:1), 1996, pp. 2-9.

Baskerville, R. "Information Systems Security Design Methods: Implications for Information Systems Development," *ACM Computing Surveys* (25:4), 1993, pp. 375-414.

Courtney, R. "Security Risk Analysis in Electronic Data Processing," in *Proceedings of the AFIPS Conference Proceedings*, National Computer Conference, Dallas, Texas, AFIPS Press, Montvale, NJ, 1977, pp. 97-104.

Dhillon, G. "Challenges in Managing Information Security in the New Millennium," in *Information Security Management: Global Challenges in the New Millennium*, G. Dhillon (ed.), Idea Group Publishing, Hershey, PA, 2001.

Dhillon, G., and Backhouse, J. "Current Directions in IS Security Research: Towards Socio-organizational Perspectives," *Information Systems Journal* (11:2), 2001.

Keeney, R. L. "Creativity in Decision Making with Value-Focused Thinking," *Sloan Management Review*, Summer, 1994, pp. 33-41.

Keeney, R. L. *Value-Focused Thinking*, Harvard University Press, Cambridge, MA, 1992.

Keeney, R. L. "The Value of Internet Commerce to the Customer," *Management Science* (45:4), 1999, pp. 533-542.

Krueger, K. H. "Internal Controls by Objectives: The Functional Control by Objectives," in *Proceedings of the IFIP/Sec '93, Computer Security: Discovering Tomorrow*, Deerhurst, Ontario, Canada, 1993, pp. 151-164.

Loch, K. D., Carr, H. H., and Warkentin, M. E. "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *MIS Quarterly*, June, 1992, pp. 173-186.

Straub, D. W., and Welke, R. J. "Coping with Systems Risks: Security Planning Models for Management Decision Making," *MIS Quarterly* (22:4), 1998, pp. 441-469.

Strens, R., and Dobson, J. "How Responsibility Modeling Leads to Security Requirements," in *Proceedings of the Sixteenth National Computer Security Conference*, Baltimore, MD, September 20-23, 1993, pp. 398-408.

Willcocks, L., and Margetts, H. "Risk Assessment and Information Systems," *European Journal of Information Systems* (3:2), 1994, pp. 127-139.