Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2007 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2007

Investigating the Development of a Multi-objective Decision Model that Seeks to Generate Informed Alternatives for Maximizing IS Security within an Organization

Jeff May
Virginia Commpnwealth University

Gurpreet Dhillon
Virginia Commonwealth University

Investigating the Development of a Multi-objective Decision Model that Seeks to Generate Informed Alternatives for Maximizing IS Security within an Organization

Jeffrey May
Virginia Commonwealth University
jmay@isy.vcu.edu

Gurpreet Dhillon
Virginia Commonwealth University
gdhillon@vcu.edu

Abstract

Numerous IS researchers have argued that IS Security can be more effectively managed if the emphasis goes beyond the technical means of protecting information resources. In an effort to adopt a broader perspective that accounts for issues that transcend technical means alone, Dhillon and Torkzadeh (2006) present an array of 9 fundamental objectives that are essential for maximizing IS security in an organization. These objectives were derived using a value-focused thinking approach and are organized into a conceptual framework. This conceptual framework provides a rigorous theoretical base for considering IS security in a manner that accounts for both technical and organizational issues, however, no current methodology exists to provide a consistent means for using these objectives so that informed decisions can be made. As a result, the goal of this paper is to investigate a means for developing a decision model that seeks to provide informed alternatives to decision makers who desire to maximize IS security within an organization.

Keywords: IS Security, Value-focused Thinking, Security Values, Multiple-objective Decision Analysis, Informed Alternatives.

Introduction

Information system (IS) security continues to present a major challenge to organizations. Currently, a number of traditional techniques are being used that attempt to provide a means for assessing and thus improving IS security. However, these traditional techniques have been shown to concentrate solely on technical matters such as confidentiality, integrity, and availability (CIA). Yet, numerous IS researchers have argued that IS Security can be more effectively managed if the emphasis goes beyond the technical means of protecting information resources (Baskerville, 1993; Hitchings, 1996; Segev et al., 1998; Straub & Welke, 1998; Armstrong, 1999; Dhillon & Backhouse, 2001; Dhillon and Torkzadeh, 2006). This new emphasis has been labeled as the socio-organizational approach (Dhillon & Backhouse, 2001) to IS security where constructs

such as ethical practices, cultural sensitivity, responsibility and awareness are considered along with the traditional constructs of CIA.

In an effort to identify IS security constructs from the socio-organizational perspective, Dhillon and Torkzadeh (2006) present an array of 9 fundamental objectives that are essential for maximizing IS security in an organization. These objectives were derived using Keeney's (1992) value-focused thinking approach and are organized into a conceptual framework. This conceptual framework provides a rigorous theoretical base for considering IS security in a manner that accounts for both technical and organizational issues, however, no methodology currently exists to provide a consistent means for assessing these objectives so that informed decisions can be made.

As a result, the goal of this paper is to investigate and propose an approach that will provide a consistent and scalable means for maximizing IS security in organizations that transcends existing technical solutions. This approach couples Dhillon and Torkzadeh's (2006) framework with multiple-objective decision analysis techniques. The future goal of such an approach is to provide a theoretically grounded methodology for generating informed alternatives to decision makers responsible for maintaining and thus maximizing IS security across multiple organizational settings,

The remainder of this paper is organized as follows. First, the current state of IS security that includes Dhillon and Torkzadeh's (2006) framework for maximizing IS security is briefly discussed. The purpose of this initial discussion is to demonstrate the need for approaching IS security from the socio-organizational perspective along with providing the need for further research in this area. After this need for further research is demonstrated, a detailed description of the proposed multiple-objective decision analysis approach that extends Dhillon and Torkzadeh's (2006) work is discussed.

Current State of IS Security

Because 75% of surveyed organizations have reported some type of IS security attack, there should be no surprise that many different traditional and widely accepted IS security methodologies exist (Bagchi & Udo, 2003). Several scholars have noted that traditional IS security methods can be classified into three distinct categories that include: checklists, risk management and formal methods (Baskerville, 1992; Backhouse & Dhillon, 1996; Siponen, 2001; Siponen, 2005). These three traditional methods are mostly technical in nature and are widely used by both scholars and practitioners. However, many researchers have noted that IS security can be more effectively handled if IS security methodologies would look beyond technical means and include various socio-organizational factors (Baskerville, 1993; Hitchings, 1996; Segev et al., 1998; Straub & Welke, 1998; Armstrong, 1999; Dhillon & Backhouse, 2001). As a result, a further IS security methodology that contains the socio-organizational perspective is currently being investigated by IS researchers. Siponen (2005) classifies this socio-organizational research under the category of soft approaches.

Checklists created for IS security assume that various security solutions and their associated procedures can be observed and turned into a functional list that can be used by practitioners (Siponen, 2005). The underlying notion is that checklists identify what can be done rather that what needs to be done (Baskerville, 1993). Typically, checklists are created by analysts who begin by determining all known security risks and control procedures available via a particular problem domain. A security checklist is then created that contains every conceivable control that can be implemented in a system. Practitioners who are responsible for maintaining security then analyze each control mechanism listed to determine if implementing such a control is required based on their knowledge of all known security risks for a particular problem domain.

Checklists offer a useful means oriented approach to implement proper security controls. Yet, checklists have been criticized by both the scholar and practitioner communities. Dhillon & Backhouse (2001) criticize checklists for their lack of theoretical stability and their lack of consideration of social problems related to security. And Backhouse & Dhillon (1996) argue, "Checklists inevitably draw concern onto the detail of procedure without addressing the key task of understanding what the substantive questions are." Practitioners have criticized checklists because the static nature of predetermined technical control can lead to security measures that do not fit the dynamic and human security requirements of an organization. For example, predetermined technical control may lead to complicated security solutions that in turn lead to poor availability of vital information (Dhillon and Torkzadeh, 2006).

The notion of risk management (RM) for IS security involves the process of measuring or assessing security risks and developing strategies to manage these risks. The methods of RM for IS security typically determine probabilities (**P**) for occurrences of particular security breaches along with the costs (**C**) associated with a given threat. Hence, the equation (**R = P * C**) is often the underlying logic of numerous IS risk management methodologies; where **R** indicates the level of risk for a particular security concern (Courtney, 1997; Baskerville, 1991).

RM for IS security is usually employed along with the use of checklists. Checklists are used to identify possible security controls, and RM techniques are used to provide a rational cost-benefit model to help eliminate unprofitable security controls (Baskerville, 1993). Clearly, there is a need to estimate the costs of implementing security controls and weighing these costs against the probability of a security breach. However, RM methodologies along with checklists have been criticized by several different scholars. For example, Clements (1977) considered RM techniques to be inappropriate for assessing IS security due to the high amount of error that is seen when coupling probability theory with the random nature of security breaches. Baskerville (1993) indicates that RM is seen as a product of guesswork because there are no reliable industry-wide statistics on which to base risk analysis. And other scholars have criticized RM because the threats and costs

associated with IS security tend to be dynamic whereas RM methods tend to be static and are based on prior knowledge (Straub and Welke, 1998; Dhillon and Torkzadeh, 2006).

Formal methods attempt to address the shortcomings of both checklists and RM approaches by dynamically managing and evaluating IS security. These methods rely on high order mathematical notations and typically concentrate on the technical considerations of confidentiality, integrity and availability (CIA) for IS security. Wing (1998) summarizes some of the major advantages of formal methods. From the designer standpoint, Wing (1998) indicates that formal methods through specification techniques help to characterize a system's behavior and properties more precisely, and through mathematical verification techniques, help to prove that a system meets its specification. However, Wing (1998) also identifies that the weakness of formal methods lies in the fact that the formal specifications of a system must always include assumptions the designer makes about the system's environment. Because environments change rapidly, often times these original assumptions that guide the formal methods no longer are correct. Additionally, clever intruders can break into a system if they can determine these assumptions. Other scholars have criticized formal methods on the basis that they rely solely on the technical considerations of CIA and do not account for socio-organizational issues (Backhouse and Dhillon, 2001).

Due to the various limitations of checklists, RM and formal methods along with the fact that they concentrate solely on technical matters, a number of scholars have called for a methodology that considers socio-organizational issues such as ethical practices, cultural sensitivity, responsibility and awareness (Baskerville, 1993; Hitchings, 1996; Segev et al., 1998; Straub & Welke, 1998; Armstrong, 1999; Dhillon & Backhouse, 2001). For example, Segev et al. (1998) state that the key to IS security "lies not with technology, but with the organization itself" (p. 85). Additionally, Trompeter & Eloff (2001) argue that organizational considerations of IS security should contain ethical and human components. And finally, Dhillon and Backhouse (2001) state, "An interpretivist understanding of information systems security concerns certainly offers advantages, furnishing a holistic view of the problem domain, especially within the scope of networked organizational forms, instead of the simplistic, one-dimensional, explanation, more suitable for hierarchically structured organizations."

Siponen (2005) argues that there have been but a few isolated attempts to approach IS security using what he calls the soft approach. For example, Straub & Welke (1998) couple interpretivist research with older form of risk analysis. Rather than assessing security risks based on probability, Straub & Welke (1998) look for semantic matches of terms specifying degrees of risk. Strens & Dobson (1993) in their research specify security requirements using explanations in terms of roles, actions, goals and policies. And Backhouse & Dhillon (1996) in their research correlated IS security concerns with organizational communication and intentional acts of agents involved, where security is regarded as an outcome of communication breakdowns. Hence, an effort has been made to examine the socio-organizational elements of IS security. However, soft approaches to IS security have inevitably been criticized due to their lack of empirical and rigorous research along with their lack of providing the IS community with a means for developing measurable socio-organizational constructs (Karyda et al., 2003; Dhillon & Torkzadeh, 2006).

Dhillon and Torkzadeh's (2006) Socio-Organizational Security Framework

In an effort to determine measurable IS security constructs from the socio-organizational perspective, Dhillon and Torkzadeh (2006) present an array of 9 fundamental objectives that are essential for maximizing IS security in an organization. Table 1 illustrates these 9 fundamental objectives that include lower tier objectives that better define each fundamental objective. These objectives were created using Keeny's (1992) value-focused thinking approach via in-depth interviews with 103 managers across various organizational settings. The results were then validated for content via a panel of seven IS security experts.

Dhillon and Torkzadeh's (2006) work answers the call to provide rigorous research that develops measurable socio-organizational constructs in the soft approach arena. As Dhillon and Torkzadeh (2006) state, "The value-focused objectives presented in this research offer a structured approach to promote systematic and deep thinking about objectives and hence assess the relative desirability of consequences." Additionally they state, "This is a significant contribution because previous research, while recognizing the importance of organizationally grounded principles, falls short of proposing tangible measures." Yet, how these objectives provide a structured approach for thinking or how these objectives could actually be measured to provide informed alternatives for decision makers responsible for maximizing IS security with an organization must be questioned.

In other words, the objectives shown in Table 1 certainly provides a theoretical template for considering IS security in a manner that accounts for both technical and organizational issues. However, without a systematic methodology or approach to provide a consistent means for assessing these objectives so that informed decisions can be made, the decision maker is forced to rely on intuition and experience alone. Thus, the accuracy of any IS security decision made in the context of these 9 fundamental objectives as they currently stand could never fully be quantified. Furthermore, when decisions are made that rely on intuition and experience alone, several heuristic biases come into play that can weaken the strength of any decision (Tversky and Kahneman, 1986; Kahneman, 2003).

As a result, further research needs to be conducted that attempts to operationalize these objectives so that informed decisions can be made for the purpose of maximizing IS security. The goal of this paper is to investigate and propose such an

approach. As will be shown in the following section, this proposed approach will couple Dhillon and Torkzadeh's (2006) framework with multiple-objective decision analysis techniques. The future goal of such an approach is to provide a theoretically grounded methodology for generating informed alternatives to decision makers responsible for maintaining and thus maximizing IS security across multiple organizational settings.

Table 1: Fundamental Objectives for Maximizing IS Security (Adapted from Dhillon and Torkzadeh, 2006)

Strategic Objective: Maximize IS Security	
First Tier	**Second Tier**
1. Enhance Management Development Practices	1.1 Develop a management team that leads by example
	1.2 Ensure individual comfort level of computers/software
	1.3 Increase confidence in using computers
	1.4 Create legitimate opportunities for financial gain
	1.5 Provide employees with adequate IT training
	1.6 Develop capability level of IT staff
2. Provide Adequate Human Resource Management Practices	2.1 Provide necessary job resources
	2.2 Create an environment that promotes contribution
	2.3 Encourage high levels of group morale
	2.4 Enhance individual/group pride in the organization
	2.5 Create an environment of employee motivation
	2.6 Create an organizational code of ethics
3. Develop and Sustain an Ethical Environment	3.1 Develop an understood value system in the organization/whistle blowing
	3.2 Develop co-worker and organizational ethical relationships
	3.3 Instill value-based work ethics
	3.4 Instill professional work ethics
	3.5 Create an environment that promotes organizational loyalty
	3.6 Stress individuals treating others as they would like to be treated
4. Maximize Access Control	4.1 Create user passwords
	4.2 Provide several levels of user access
	4.3 Ensure physical security
	4.4 Minimize unauthorized access to information
5. Promote Individual Work Ethic	5.1 Maximize employee integrity in the company
	5.2 Minimize urgency of personal gain
	5.3 Create a desire to not jeopardize the position of the company
	5.4 Create an environment that promotes company profitability rather than personal.
	5.5 Minimize temptation to use information for personal benefit
6. Maximize Data Integrity	6.1 Minimize unauthorized changes
	6.2 Ensure data integrity
7. Enhance Integrity of Business Processes	7.1 Understand the expected use of all available information
	7.2 Develop understanding of procedures and codes of conduct
	7.3 Ensure that appropriate organizational controls (formal and informal) are in place
8. Maximize Privacy	8.1 Emphasize importance of personal privacy
	8.2 Emphasize importance of rules against disclosure
9. Maximize Organizational Integrity	9.1 Create an environment of managerial support and solidarity
	9.2 Create environment of positive management interaction
	9.3 Create an environment that promotes respect
	9.4 Create an environment that promotes individual reliability
	9.5 Create environment of positive peer interaction

Developing a Decision Model that Seeks to Maximize IS Security within an Organization

Dhillon and Torkzadeh's (2006) framework of fundamental objectives for maximizing IS security was created using original ideas from Keeney's (1992) value-focused thinking approach. The value-focused thinking approach was derived from the field of Operations Research and offers a robust means for making decisions (Clemen, 1996). Keeney (1992, p. 3) indicates that there are two primary methods of thinking about decisions: alternative-focused thinking (AFT) and value-focused thinking (VFT). Figure 1 illustrates the difference between AFT and VFT. As shown in Figure 1, AFT, the classical decision-making technique, lists "identify alternatives" as the second step in the decision making process once the problem

has been identified. Keeney (1992, p. 6) criticizes AFT because it tends to constrain a decision maker to a generated set of existing alternatives that often times do not reflect what is truly important for a decision. Additionally, once alternatives are determined, the decision maker is often times "anchored" (Kahneman, 2003) to this domain thus limiting the decision-makers ability to consider alternatives outside of this box (Keeney, 1992, p. 48). In contrast to AFT, VFT first determines the values inherent to any decision context and then proposes finding creative alternatives that can adequately address these values.

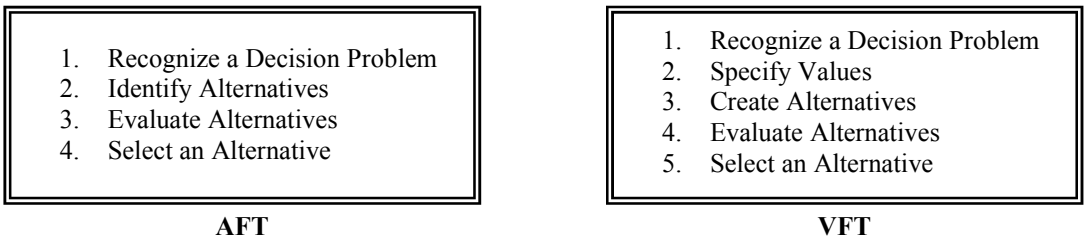

Figure 1: AFT versus VFT

For example, if a decision maker is tasked with determining the best way to maximize IS security within an organization, a list of alternatives might include checklists, risk management and formal methods. Using the AFT approach, the decision maker would then proceed to determine which of these alternatives would be best for her organization and would then implement one of these alternatives without considering the underlying values inherent to this decision context. Any solution that is implemented would thus be bounded to the constraints of the chosen alternative. In contrast, VFT ensures that the decision maker first figures out what is needed in the form of values and then determines the appropriate alternatives that truly address these needs. In other words, VFT recognizes that alternatives should be the means for achieving the more fundamental and often times hidden values that lie below any decision context.

Dhillon and Torkzadeh's (2006) framework shown in Table 1 instantiates the first 2 steps of the VFT process shown in Figure 1 and provides the IS research community with a theoretical framework for addressing IS security from the socio-organizational perspective. However, without providing a methodology for creating, evaluating and selecting alternatives, the results of their exhaustive research efforts are limited in their practical capacity to provide decision-makers with the ability to make informed decisions. Thus further research is required to develop methodologically sound techniques for creating, evaluating and selecting the best alternatives in the context of maximizing IS security within an organization.

To generate informed alternatives from multiple objectives, a number of both qualitative and quantitative techniques can be used. One technique known as the analytic hierarchy process (AHP) has been developed for these types of problems (Saaty, 1980). In short, the AHP is a mathematical decision making technique that allows consideration of both qualitative and quantitative aspects of decisions. It reduces complex decisions to a series of pairwise (one-on-one) comparisons then synthesizes the results. However, AHP suffers from shortcomings in the area of consistency and rank reversals and can be difficult to implement with a large number of alternatives (Chambal et al., 2003).

To generate informed alternatives for the purpose of maximizing IS security this paper proposes using a 10-step methodology as shown in Table 2. This step-by-step methodology combines both qualitative and quantitative techniques and was derived from the multi-objective decision analysis literature (Keeney, 1992; Keeney and Raiffa, 1993; Kirkwood, 1997; Chambal et al., 2003). Other researchers have used similar approaches for solving various problems outside the IS domain. For example, Chambal et al. (2003) used this methodology to provide decision-makers with a decision aid for choosing a new municipal solid waste management strategy. And Merrick and Garcia (2004) used a similar approach to provide decision-makers with the best alternatives for improving a particular watershed.

Table 2: Proposed 10-Step Research Approach

Step	Activity	VFT Process	Notes
1	Define a Strategic Objective	Recognize a Decision Problem	Dhillon and Torkzadeh (2006)
2	Create Value Hierarchy	Specify Values	Dhillon and Torkzadeh (2006)
3	Develop Evaluation Measures	Evaluate Alternatives	Case Study - SM, M, and O
4	Create Value Functions	Evaluate Alternatives	Case Study - SM
5	Weight the Value Hierarchy	Evaluate Alternatives	Case Study - SM
6	Generate Alternatives	Create Alternatives	Case Study -SM, M, and O
7	Score Alternatives	Evaluate Alternatives	Case Study - SM
8	Rank Alternatives	Evaluate Alternatives	Researcher
9	Perform Sensitivity Analysis	Evaluate Alternatives	Researcher
10	Recommendations	Select an Alternative	Researcher

SM = Strategic Managers; M = Managers, O = Operational Employees

As shown in Table 2, the first 2 steps of this research approach have already been addressed by Dhillon and Torkzadeh (2006). Thus, this research proposes extending their research to account for Steps 3-10 using an additional organizational case study. For the purposes of this proposed research, the organization chosen should be broken down into strategic, managerial, and operational elements. The bulk of this case study would then be spent with the strategic managers (decision-maker (DM)) of an IS department who are responsible for maintaining security within their organization. As will be shown, the managerial and operational employees of the entire organization will then be probed in the form of questionnaires to develop a better understanding of how the organization rates on various evaluation measures. Additionally, the managerial and operational employees will also be asked to generate alternatives that come to mind as a result of considering various evaluation measures. The remainder of this paper will be spent discussing Steps 2–10 shown in Table 2 in more detail in the context of this proposed case study.

Step 2 - Create a Value Hierarchy

A value hierarchy is used by the decision maker as a conceptual model for generating alternatives. It structures the organizational values beginning with the strategic objective and ending with lower level objectives used during the evaluation process. Fundamental objectives are those that a decision maker actually desires to achieve in the context a particular problem domain. A hierarchy of fundamental objectives can then be developed as a tree with lower tier objectives serving to define in more detail what is meant by higher tier objectives. A value hierarchy ensures that the fundamental objectives are appropriately related to the strategic objective (Kirkwood, 1997) and aids an organization in identifying whether any values are missing or if any additional values are needed (Keeney, 1992).

The process for generating a value hierarchy in terms of eliciting values from interviewees and how to structure these values is detailed by Keeney (1992) and was followed closely by Dhillon and Torkzadeh (2006) to generate the objectives hierarchy shown in Table 1. Desirable properties for an objectives hierarchy include completeness, nonredundancy, decomposability, operability, and small size (Kirkwood, 1997). The *completeness* or "collectively exhaustive" property refers to the notion that the objectives at each tier in the hierarchy must adequately cover all concerns necessary to evaluate the upper level objective and assures that alternatives are adequately evaluated and ranked accordingly. The *nonredundancy* or "mutually exclusive" property implies that no two objectives in the same tier of the hierarchy should have the same or similar meanings. The *decomposability* property refers to the notion that there must be a way to measure each objective in order to determine the overall desirability of alternatives. The *operability* property refers to the notion that the objectives hierarchy should be understandable for the people who will be using it. And the *small size* property refers to the notion that the hierarchy should be no bigger than necessary to minimize the duration of time spent on each of the downstream steps of the 10-step methodology shown in Table 2.

When investigating the objectives shown in Table 1 against the desirable properties of any value hierarchy the property of *decomposability* appears to be problematic. In other words, determining measures for the second tier objectives will be challenging because the qualitative nature of these objectives do not readily allow for direct measurement. Thus, creating a sound technique for measuring these objectives must be investigated with care. Additionally, it should be noted that because the fundamental objectives shown in Table 1 were generated via multiple organizational settings, then it will be assumed that this framework can be deemed generalizable to any organizational setting that desires to maximize IS security.

Step 3 - Develop Evaluation Measures

Once the value hierarchy is created, one or more evaluation measures or metrics (AKA attributes) must be developed for each of the objectives in the last tier of each branch in the hierarchy. The purpose of evaluation measures is to specify an unambiguous rating of how well an alternative does with respect to each objective (Kirkwood, 1997). An evaluation measure may have either a natural scale that can be measured directly or a constructed scale that is either measured directly or indirectly (proxy scale). A natural scale that can be measured directly has a common interpretation to everyone and is thus less controversial (Keeney, 1992; Kirkwood, 1997). For example, the concentration of chlorine in a water column is typically measured using mg/l and can be directly measured. In contrast, a constructed scale is developed specifically for a given decision context. For example, survey questions that use a 5-point Likert rating would be considered a constructed scale.

As shown in Table 1, the qualitative nature of the second tier objectives may not allow for natural measurement. Thus constructed scales must be developed for the purposes of this research. This paper proposes developing an exhaustive list of generic questions (questionnaire) to measure each of the second tier objectives shown in Table 1. These generic questions will then be presented to the DM where the goal would be to form a more accurate set of questions and scales (i.e., 5-point Likert) that relate to the DM's specific organizational context. In addition to developing accurate, organizationally

specific questions, this process would also provide the DM with a first and detailed view of the value hierarchy so that later analysis via these objectives will be less strenuous.

For each second tier objective, the questions created will be administered to both managerial and operational employees. For example a managerial measure for objective 1.1 shown in Table 1 might be, "You and your management team attempt to develop an environment that leads by example." To administer these questions, a computer program will be created that will allow respondents to answer questions online and will subsequently store results in an appropriately designed database.

Step 4 - Develop Value Functions

Typically, the evaluation measures developed in the previous step are in different units and measured on different scales. Thus as Keeney (1992) notes, it is impossible to sum the individual measurements to obtain a total score. To solve this problem, value functions must be developed to transform the units of each evaluation measure into "value units" on a scale of 0 to 1 (Kirkwood, 1997).

For this research it may be found that using a 5-point Likert scale would be appropriate for measuring many of the second tier objectives shown in Table 1. Yet, whether or not the differences between each point on the Likert scale have the same difference in value must be investigated for each measure by soliciting the DM's experience and judgment. That is, if differences in each point on the Likert scale are assumed to be the same, then the assignments of values shown in Table 3 could be given for each score. However, if it is determined that various questions do not have an equal change in value then an alternative technique must be employed.

Table 3: Values for Evaluation Measures Assuming Equal Change in Value

Score	Meaning	Value
1	Strongly disagree	0
2	Disagree	0.25
3	Neither agree nor disagree	0.5
4	Agree	0.75
5	Strongly agree	1

For example, consider the question "You and your management team attempt to develop an environment that leads by example." After discussing this measure with the DM, it might be found that a bigger difference between a score of 3 and 4 and 3 and 2 exists than it does for a score of 4 and 5 and for 1 and 2. Thus, the value function would look more like that shown in Figure 2 rather than being a straight line. Additionally, within a particular value model, value functions are preferred to be either all monotonically increasing or all monotonically decreasing to establish consistency (Chambal et al., 2003). For example, a monotonically increasing value function means that the score along the x-axis increases as the value along the y-axis also increases. Subsequently, a value model having value functions that are all monotonically increasing aids those responsible for scoring the alternatives because they will know that "more is always better" when considering evaluation measures. As a result, this research proposes developing evaluation measures that lead to monotonically increasing value functions.

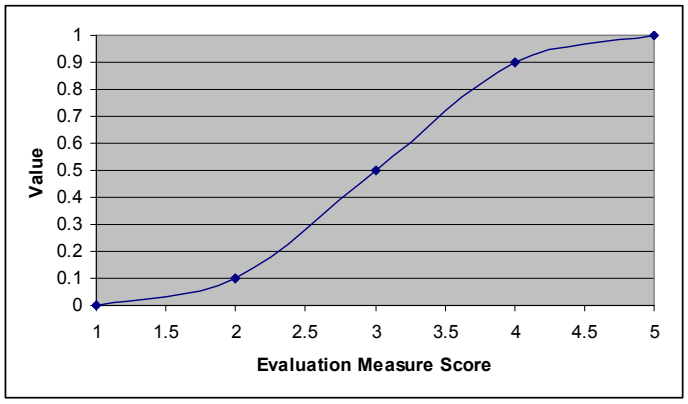

Figure 2: Values for Evaluation Measures with Non-Equal Changes in Value

The process for determining non-linear value functions is detailed by Kirkwood (1997, pg.62). The process consists of first setting the lowest and highest evaluation measure scores to values of 0 and 1, respectively. The DM is then asked to consider if there is any differences in value when going from 1 to 2, 2 to 3, 3 to 4, and 4 to 5. Perhaps the DM might then indicate that the difference in going from 5 to 4 is much less than going from 4 to 3 for a particular evaluation measure and that this difference is approximately 4 times as great. Additionally, the DM might indicate that the same is true on the lower end. Thus the researcher would then set the lowest increments from 1 to 2 and 4 to 5 to $\boldsymbol{x}$ and the increments from 2 to 3 and 3 to 4 to $4\boldsymbol{x}$. The value of $\boldsymbol{x}$ could then be solved by recognizing that $\boldsymbol{x} + 4\boldsymbol{x} + 4\boldsymbol{x} + \boldsymbol{x} = 1$; or $\boldsymbol{x} = 0.1$. The values for each evaluation measure could then be determined as shown below and would then generate the value function shown in Figure 2.

$$V(5) = \boldsymbol{x} + 4\boldsymbol{x} + 4\boldsymbol{x} + \boldsymbol{x} = 1.0;\ \boldsymbol{x} = 0.1$$

$$\therefore \quad V(1) = 0$$
$$V(2) = \boldsymbol{x} = 0.1$$
$$V(3) = \boldsymbol{x} + 4\boldsymbol{x} = 0.5$$
$$V(4) = \boldsymbol{x} + 4\boldsymbol{x} + 4\boldsymbol{x} = 0.9$$

Step 5 – Weight the Value Hierarchy

The value hierarchy is composed of multiple objectives that should be considered when attempting to make a decision. However, each of these objectives is not necessarily equally important to a particular decision-maker across various organizations. Therefore, to account for this varying degree of importance, weights must be assigned to each tier of the value hierarchy given a particular organizational context. An important property of the hierarchy is that the local weights for each branch and each tier, taken separately, must sum to 1.0.

Several weighting techniques exist that include: the ratio method, the swing weighting method, the trade off method, and the pricing out method (Borcherding et al., 2003). This paper proposes using the swing weighting technique as it has been shown to be a consistent technique that provides a fair amount of convergent validity (Borcherding et al., 2003). In using swing weights the DM (or DMs) within a particular organization will be asked to imagine the lowest tier objectives for each branch at their worst possible levels in terms of value. They will then be asked to determine which objective in a group they would like to see swing to its best possible level. After choosing their most important objective within a group, they will then be asked to compare their two most important objectives and state the relative importance of a full swing in each objective's attainment. After a few iterations of this technique, the researcher would then be able to determine the various increments between each objective. The resulting increments are then sequentially ordered by increasing value. Each increment is then assigned a factor of importance as it relates to the smallest increment. The smallest value increment is then set so that the total of all the increments equals 1. The resulting increments that sum to one are then solved as a system of equations in the exact manner as shown in Step 4 above with the same number of equations and unknowns to produce the various weights. If more than one DM is solicited for determining weights, the various weights produced will then be combined and averaged to provide a final weight for each objective and evaluation measure at each tier of the hierarchy.

Step 6 - Generate Alternatives

The major advantage of VFT is that it encourages the development of creative alternatives, guided by the knowledge of the organizational values (i.e., the value hierarchy shown in Table 1). Depending on the situation, there are different techniques for actually generating the alternatives. To generate alternatives, the value hierarchy forces appropriate value driven questions to be asked to accurately assess and measure the various evaluation measures for the various objectives. Thus, when administering the online questionnaire as discussed in Step 3 above, each question will be followed up with a question that elicits alternatives from the various respondents for improving upon any given objective. After this exhaustive list is compiled, these alternatives will then be discussed with the DM to determine if any additional alternatives that address various objectives should be added.

Step 7 – Score the Alternatives

For the purposes of creating a value model the alternatives generated in Step-6 must be scored relative to each evaluation measure. That is, each alternative will receive a score in the range of possible values for each evaluation measure. To determine these scores, a forum of subject matter experts (researcher, DM, outside experts) considers each alternative for a particular measure before advancing to the next measure. Ideally, the forum of subject matter experts arrives at a consensus for each score an alternative receives. This consensus adds defensibility to the final value ranking of the alternatives because it eliminates the uncertainty factor associated with each score an alternative receives. If the situation arises where a particular

alternative negatively impacts a particular objective, negative scores may need to be considered and value functions would have to be amended for these cases. Additionally, given the high degree of mutually exclusive objectives shown in Table 1, individual alternatives will probably only impact a small number of individual objectives. Thus, the time required to accurately complete Step 7 will not be too overwhelming.

Step 8 - Perform Deterministic Analysis

As shown in Table 1, 39 second tier objectives will be measured where over 100 evaluation measures might be needed that could possibly generate over 100 alternatives. Thus, the next question becomes which of these alternatives would have the most impact on maximizing IS security for a particular organization? The goal of deterministic analysis is to allow the various alternatives to be ranked in order of importance and will provide an informed and quantifiable means for justifying alternative selection.

To perform deterministic analysis, the data collected in the previous steps will be used to create an overall value function. There are several approaches for creating overall value functions where the additive and multiplicative value functions are the most commonly used (Chambal et al., 2003). Because the additive value function is particularly salient for prescriptive decision analysis, it will be used as a basis for this research. The additive value function assumes each single-dimensional value function contains a value of 0 for the worst level and a 1 for the best level (monotonically increasing) and that that alternatives are preferentially independent (Keeney and Raiffa, 1993). The preferential independence property essentially indicates that the choice of a particular alternative does not impact other alternatives. With these assumptions, the additive value function is simply a weighted average of all of the various value functions and is expressed as shown in Equation 1 (Kirkwood (1997, pg. 230):

$$(1)\quad v(x) = \sum_{i=1}^{n} w_i * v_i(x_i)$$

where w_i = the various weights associated with the various alternative scores via the value functions $v_i(x_i)$.

Table 3 illustrates (using fictitious numbers for the purpose of illustration) how this deterministic analysis will be accomplished using the sixth branch ("Maximize Data Integrity") of the value hierarchy shown in Table 1. As mentioned in Step 5, the 3 weight columns would be generated using the swing weighting technique via interviews with DMs. The adjusted weight (AW) column (AKA: global weight) would then be calculated as W1 * W2 * W3. The measure column represents the list of evaluation measures that will be generated and asked via the proposed online computer survey. The average-adjusted-score (AAS) column then represents the average value of the combined scores of all respondents adjusted via the value function scheme shown in Step 4. This column represents how the organization did with respect to a particular evaluation measure. The scaling factor (SF) column then represents the importance of a particular measure and is calculated as 1 – AAS. That is, the higher the SF the more room there is for improvement of a particular objective. The alternatives column (Alt) would be the actual alternatives generated via the online questionnaire and subsequent post questionnaire interviews with the DMs. The score column is the actual score of each alternative relative to each measure as discussed in Step 7. And finally, the value adjusted score column (VAAS) is the score adjusted via the value functions created in Step 4.

Table 3: Table for Deterministic Analysis

First Tier		Second Tier		Third Tier Evaluation Measures					Alternatives		
Objective	Weight (W1)	Objective	Weight (W2)	Measure	Weight (W3)	Adj. Weight (AW)	Avg. Adj. Score (AAS)	Scaling Factor (SF)	Alt	Score	Value Adj. Score (VAAS)
6	0.2	6.1	0.25	Q6.1.1	0.5	0.025	0.67	0.33	A1	4	0.9
									A2	5	1
				Q6.1.2	0.5	0.025	0.33	0.67	A2	3	0.5
									A3	4	0.9
		6.2	0.75	Q6.2.1	0.5	0.075	0.23	0.77	A3	2	0.1
				Q6.2.1	0.5	0.075	0.89	0.11	A2	3	0.5
									A4	4	0.75
Step	*Step*	*Step*	*Step*	*Step*	*Step*	*Step*	*Step*	*Step*	*Step*	*Step*	*Step*
2	*5*	*2*	*5*	*3*	*5*	*5*	*8*	*8*	*6*	*7*	*8*

The following calculations represent the final step in determining the best alternatives using Equation 2 (derived from Equation 1) and the values shown in Table 3. Thus as is shown by these equations the alternatives A_2 and A_3 would be recommended as they would have the greatest impact on increasing the overall strategic objective of maximizing IS security.

$$(2): \; V(A_i) = 1000 * \sum_{i=1}^{n} SF_i * AW_i * VAAS_i$$

$$\therefore \quad V(A_1) = 1000*(0.025)(0.33)(0.9) = \mathbf{7.4}$$
$$V(A_2) = 1000* [(0.025)(0.33)(1.0) + (0.025)(0.67)(0.5) + (0.075)(0.11)(0.5)] = \mathbf{20.8}$$
$$V(A_3) = 1000* [(0.025)(0.67)(0.9) + (0.075)(0.77)(0.1)] = \mathbf{20.\ 9}$$
$$V(A_4) = 1000* (0.075)(0.11)(0.75) = \mathbf{6.2}$$

Steps 9 and 10 - Perform Sensitivity Analysis and Present Final Recommendations

After the deterministic analysis is completed, the next step is to perform sensitivity analysis. This procedure is recommended as it examines the validity of the findings by removing the subjective nature of the weights and often times provides the DM with valuable insight. In other words, sensitivity analysis may be of interest to a DM because of the potential disagreement between stakeholders regarding the weights and the affect that these weights may have on the final ranking of the alternatives. To accomplish this analysis, the weight of each value is systematically altered and the subsequent impact on the final alternative scores and rankings are tracked. As an individual weight is changed, the other weights are adjusted to ensure that the sum of the column or section remains one. The proportionality of the other weights to each other is maintained as the weight being assessed is adjusted.

Once the sensitivity analysis is complete, final recommendations are presented to the DM. The format of the presentation depends on the insights gained during the analysis and the questions posed by the DM. It is important to communicate that this 10-step VFT process does not replace the DM; it only serves as a structured approach that serves as a guide to generate informed alternatives derived from the values inherent to any decision context.

Conclusions

This paper examined the current state of IS security and documented some shortcomings of traditional IS security practices such as checklists, risk management and formal methods. In short, due to the fact that these traditional techniques have been shown to concentrate solely on technical matters, a broader perspective that accounts for socio-organizational issues was found to be more appropriate when considering IS security.

This paper then examined Dhillon and Torkzadeh's (2006) theoretical framework of 9 fundamental objectives for maximizing IS security in an organization. These objectives were derived using a value-focused thinking approach and illustrate that both technical and socio-organizational issues are indeed valued by decision-makers responsible for maintaining IS security. Dhillon and Torkzadeh's (2006) framework provides a rigorous theoretical base for considering IS security from the socio-organizational perspective. Yet, no current methodology exists that seeks to assess these objectives so that informed decisions can be made in the context of IS security.

As a result, this paper investigated the use of a 10-step methodology that seeks to discover and select the best alternatives that relate to maximizing IS security in any given organizational setting. This methodology was derived from the multi-objective decision analysis literature stream and if used in future case study research could provide meaningful insight to three areas. First, from a theoretical standpoint, this methodology could offer further specification and refinement to Dhillon and Torkzadeh's (2006) theoretical framework. Second, from a practical standpoint, this methodology could lead to the creation of decision models and auditing tools that account for both technical and socio-organizational issues in the context of maximizing IS security across multiple organizations. And finally, successful implementation of this methodology in the context of IS security would thus allow it to become a prime candidate for solving other IS related problems where both qualitative and quantitative issues exist.

References

Armstrong, H. (1999). "A soft approach to management of information security." School of Public Health. Curtin University. Perth, Australia, Unpublished PhD Thesis 343.

Backhouse, J. and G. Dhillon (1996). "Structures of responsibility and security of information systems." *European Journal of Information Systems* 5(1): 2-9.

Bagchi, K. and G. Udo (2003). "An analysis of the growth of computer and Internet security breaches." *Communications of AIS* 12, 684–700.

Baskerville, R. (1991). "Risk analysis: an interpretive feasibility tool in justifying information systems security." *European Journal of Information Systems* 1(2): 121-130.

Baskerville R. (1992). "The developmental duality of information systems security." *Journal of Management Systems* 4(1), 1–12.

Baskerville, R. (1993). "Information systems security design methods: implications for information systems development." *ACM Computing Surveys* 25(4): 375-414.

Bell, D. and LaPadula, L.. (1973). "Secure computer systems: Mathematical foundations." Technical Report ESD-TR-73-278, The MITRE Corporation, Bedford, MA.

Borcherding, K., Eppel, T., and Von Winterfeldt, D., (1991). Comparison of Weighting Judgments in Multiattribute Utility. *Management Science*, 37, 12, 1603 – 1619.

Chambal, S., Shoviak, M., and Thal, A. E. (2003). "Decision Analysis Methodology to Evaluate Integrated Solid Waste Management Alternatives." *Environmental Modeling and Assessment* 8: 25-34.

Clemen, R. T. (1996). *Making Hard Decisions: An Introduction to Decision Analysis* (2nd edition). Belmont, CA: Duxbury Press.

Clements, D. P. (1977). Fuzzy ratings for computer security evaluation. University of California, Berkeley. Unpublished PhD Thesis.

Courtney, R. (1997). "Security risk analysis in electronic data processing." Proceedings of the AFIPS, pp. 97 – 104.

Dhillon, G. and J. Backhouse (2001). "Current directions in IS security research: towards socio-organizational perspectives." *Information Systems Journal* 11(2): 127-153.

Dhillon, G. and G. Torkzadeh (2006). "Value focused assessment of information system security in organizations." *Information Systems Journal.*

Hitchings, J. (1996). A practical solution to the complex human issues of information security design. *Information systems security: facing the information society of the 21st century*. S. K. Katsikas and D. Gritzalis, (Ed.). London, Chapman & Hall: 3-12.

Kahneman, D. (2003). "A perspective on judgment and choice: Mapping bounded rationality." *American Psychologist, 58,* 697-720.

Karyda, M., S. Kokolakis and E. Kiountouzis (2003). Content, context, process analysis of IS security policy formulation. *Security and privacy in the age of uncertainty*. D. Gritzalis, S. D. C. d. Vimercati, P. Samarati and S. Katsikas, (Ed.). Boston, Kluwer Academic Publishers: 145-156.

Keeney, R. L. (1992). *Value-focused thinking*. Cambridge, Massachusetts, Harvard University Press.

Keeney, R. L. and Raiffa, H. (1993). *Decsions with Multiple Objectives*. Cambridge, Massachusetts, Cambridge University Press.

Kirkwood, Craig W. (1997). *Strategic Decision Making, Multiobjective Decision Analysis with Spreadsheets*. Belmont: Wadsworth Publishing Company.

Merrick, J. R. and Garcia, M. W. (2004). "Using Value-Focused Thinking to Improve Watersheds." *Journal of the American Planning Association* 70(3): 313 – 337.

Saaty, T. (1980). *The Analytical Hierarchy Process.* NY, NY, McGraw-Hill, International.

Segev, A., J. Porra and M. Roldan (1998). "Internet security and the case of Bank of America." *Communications of the ACM* 41(10): 81-87.

Siponen, M. T. (2001). "An analysis of the recent IS security development approaches: descriptive and prescriptive implications." *Information security management: global challenges in the new millennium*. G. Dhillon, (Ed.). Hershey, Idea Group Publishing: 101-124

Siponen, M. T. (2005). "An analysis of the traditional IS security approaches: implications for research and practice." *European Journal of Information Sytems* 14(10): 303-315.

Straub, D. W. and R. J. Welke (1998). "Coping with systems risks: security planning models for management decision making." *MIS Quarterly* 22(4): 441-469.

Strens, R. and Dobson, J. (1993). "How responsibility modeling leads to security requirements." *Proceeding of the 16th National Computer Security Conference*, Baltimore, MD, pp. 398 – 408.

Tversky, A., and Kahneman, D. (1986). "Rational choice and the framing of decisions." *Journal of Business, 59,* S251–S278.

Trompeter, C. M. and J. H. P. Eloff (2001). "A framework for implementation of socio-ethical controls in information security." *Computers & Security* 20(5): 384-391.

Wing, J. M. (1998). A Symbiotic Relationship between Formal Methods and Security. Proceedings from Workshops on Computer Security, Fault Tolerance, and Software Assurance: From Needs to Solution. CMU-CS-98-188, December.