2004

Decision Support in Information Systems Security

Omar F. El-Gayar
Dakota State University

Brian D. Fritz
Dakota State University

Decision Support in Information Systems Security

Omar F. El-Gayar College of Business and Information Systems Dakota State University Omar.el-gayar@dsu.edu	Brian D. Fritz College of Business and Information Systems Dakota State University fritzb@pluto.dsu.edu

ABSTRACT

As the structure of modern organizations shifts, so correspondingly must the methodologies which underlie the evaluation and development of the security posture of their information systems. We have witnessed an ever-growing gap between organizational policy and technology. We have also witnessed an ever increasing complexity of decisions regarding the planning and design of IS security.

Within this paper, we propose a decision support framework consistent with security and decision theory and develop a model of the decision analysis space suitable for multiple criteria decision making (MCDM). The adoption of MCDM techniques within the context of this model can show inherent trade-offs between alternatives in a security decision, encapsulate qualitative as well as quantitative elements within the analysis space, and facilitate group-decision making thereby dealing with conflicting perspectives of multiple stakeholders. The paper concludes with a demonstration of the proposed model through a case study conducted with a major financial services provider.

Keywords

Information systems security planning, design, and management; Decision support; Multiple criteria decision making

INTRODUCTION

A recently conducted study (Whitman, 2003) indicates that 99% of companies surveyed utilize the Internet for purposes ranging from providing information to ordering and value-chain integration with business partners. Yet an astonishingly low 63% of these organizations indicated that they possess a consistent security policy. A major study conducted by the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI) indicated that over 90% of organizations surveyed had faced systems security related incidents in the past year, and estimated total financial losses from such incidents at $455,848,000 (Power, 2002). It is quite obvious that information systems (IS) security is becoming a critical issue which can directly impact on many aspects of business operations, and that security violations are indeed occurring and resulting in real losses.

The rapid technology- and market-driven changes which have characterized the shifting business horizon as pertains to organizational structures and the technical environment have created a need for corresponding flexibility in such organizations' ability to ascertain and understand the changing nature and conditions of the security of their information systems. Too often, security is treated by top management as largely a technical concern. Often, this attitude results in overly generalized policies with a systematic effect characterized by an ever-widening gap between policy and technology, and a corresponding disconnection between decision-makers and technical management (Baskerville and Siponen, 2001; Ferris, 1994) within the organization.

Increasingly, the sheer volume of specialist knowledge necessary to a purely functional security approach is overwhelming. Moreover, a multitude of factors may be involved which concern the value and significance of a particular asset to an organization. These factors may be entirely non-technical in nature, or qualitative and subjective. Unfortunately, existing methodologies for security decision-making offer limited options and are tailored to the technical problems of identifying assets and matching threats to controls, and provide virtually no support for evaluating trade-off among various factors.

It is our contention that multi-criteria decision making (MCDM) techniques can be usefully applied to this problem domain to significant advantage over traditional security management approaches, in eliciting stakeholder preferences, explicitly showing trade-offs inherent in security decisions, and dealing with conflicting priorities between stakeholders. We contend

that such decision support techniques can be utilized to improve managerial perception of security and in turn to facilitate development of correct notions of the organization-wide significance of security, and to provide a sound theoretical basis for formulating security decisions.

Within this paper, we extend the existing literature on decision support for information security planning to develop a framework of the decision process itself, consistent with security and decision theory, and identify within the framework the specific portions of the process where decision support techniques can be utilized. From this, we then develop a model of the decision analysis space suitable for MCDM that incorporates the traditional security categories of threat, asset, and control, and show how this model may be used to describe analysis spaces useful to security management. We conclude with a case study conducted through use of a sample application of the model in consultation with a major financial services provider.

INFORMATION SYSTEMS SECURITY DECISIONS

Traditionally, information systems security has been considered an issue of import primarily to the IT department of an organization (Dhillon and Backhouse, 2000). It has consistently been the case that the organization-wide importance of information security has been all but ignored by IT management and top executives (Whitman, 2003). Oftentimes, managers also lack the technical knowledge necessary to communicate organizational concerns in a way that has relevance to operational personnel, and fail to treat security problems as an ongoing concern (Wood, 1997). Security is treated as a specialized technical matter, left to the responsibility of the IT department. Treatment of security as a purely technical concern is the result of the traditional view of information security as the responsibility of the IT department, combined with a lack of grounding in theoretical principles of security management and insufficient knowledge of managerial security controls (Straub and Welke, 1998).

Current security planning techniques involve primarily a combination of two aspects: policy making, which is intended to give strategic direction to information security efforts, and operational procedures and implementation, which supplies an essentially tactical function to the organization, and which is very much slanted towards specific behavioral regulations and the technical aspect of security. Unfortunately, in practice, as well as the security literature, we see a widespread discontinuity between these two aspects. Too often, what is characterized as an ad-hoc approach to security planning (Rees et al., 2003; Gaskell, 2000) predominates, wherein there is little concern beyond that raised by the publicity generated by the latest security breach which is brought to managerial attention, often without an understanding of the true significance of the publicized threat to a particular organization.

Implemented policies are often generalized and intended to give broad direction, but too frequently, this result in fundamentally ineffective security policy with little operational relevance, which fails to remain timely with changes in the security environment, and which is inconsistent with and irrelevant to strategic objectives (Rees, Banyopadhyay, and Spafford, 2003). The lack of a mediating influence between awareness of publicized vulnerabilities and the impact of such vulnerabilities on the individual organization's security posture also has undue influence on decision-making. It can result in fundamentally reactive security decisions, wherein there is little concern beyond prevention of the latest publicized breach serving as a model guiding future actions (Rees et al., 2003).

Policy-based techniques have identified and sought to alleviate this problem through suggestions for establishment of meta-levels of policy (Baskerville and Siponen, 2002), and broad and comprehensive guidelines and models have been presented, many derived from experience through military and governmental use. Such guidelines and meta-policies for development of security policy may be useful to an organization for improving its policy making process, but alone they do not adequately address the real "gap" – that of communication between upper management and operational IT security management – which exists in the security decision process between security planning and implementation.

Perception of IT-related risk, including information security, can vary greatly from the theoretical concepts of probability theory used to quantify the possibility of future outcomes. These perceptions, of course, form the basis for consequent future decisions. It has been shown that managers are largely unaffected by probability estimates and tend to consider a "risky" choice as one which might have a very negative outcome, regardless of its actual probability of occurrence (March and Shapira, 1987) – thus the ordinary managerial decision process cannot be considered to be governed by statistical evaluation methods common to risk management theory. As Bandyopadhyay, Mykytyn, and Mykytyn (1999) conclude, IS managers need to change their way of thinking about risk.

In effect, a security decision consists of eliciting the values, preferences, and priorities of the stakeholders in the decision, and in understanding how the trade-offs between potential alternatives will affect the extent to which the choice is able to achieve the objective of the decision. Accordingly, security decisions are amenable to techniques suitable for making decisions in the presence of multiple, and often conflicting criteria.

Such techniques are referred to as multiple criteria decision making techniques (MCDM). Multi-criteria decision making (MCDM) is a research area in decision theory which is intended to account for multiple attributes and criteria in the decision-making process. MCDM encompasses a wide variety of techniques, and classically it is considered to incorporate the economic paradigm, advanced by Von Neumann and Morgenstern (1944), of expected utility theory applied to multiple criteria. Multi-attribute utility theory (MAUT), as a representative example of a class of such techniques, utilizes this notion explicitly in the decision process (Olson, 1996). An MCDM approach can facilitate systematic thinking about the problem domain, through its provision of a framework for defining alternatives and comparing their performance in chosen objectives (Thomas and Samson, 1986). Additionally, MCDM methods are well-suited to issues which can arise in group decision making, including conflicting evaluations of trade-offs and multiple divergent viewpoints.

MCDM also facilitates negotiation, because it serves to move the discussion away from the specific alternatives under discussion and focus the process towards understanding the values underlying the overall decision objectives and clearly illustrating the trade-offs between alternatives. This encourages stakeholders to consider their common interests and to mitigate the effect of defensive dispute, which often occur after a stakeholder is invested in a particular alternative (Raiffa, 1982). Discussions based on value also can serve as sources of new and unconsidered alternatives (Gregory and Keeney, 1994). These discussions naturally lead themselves to support of strategic and holistic thought about a problem domain, and thus MCDM methods can serve to address less quantifiable policy-based objectives and to show directly how existing factors within an organization lend themselves to support these broader, directive goals.

While MCDM techniques have been applied extensively in various application domains, their application in the management and planning of information system security is almost non-existent. Available tools and methods for security risk planning rely on simplistic techniques that ignore behavioral aspects entirely and cannot account for the multidimensional effects of controls (Straub and Welke 1998), they are atheoretical (Hoffman 1989), and they do not facilitate the type of decision making involving cross-functional organizational components which are characteristic behaviors of a modern emergent organization as it is described by Baskerville and Sipponen (2001). These techniques are biased toward what is characterized in the literature as a technocratic orientation (Willison, Backhouse 2003). Baskerville (1993) presents a review of some of the information system security design methods in the context of information system development.

A DECISION SUPPORT FRAMEWORK OF THE SECURITY DECISION PROCESS

The security decision process itself can be characterized as a case of the general theoretical model for decision-making advanced by Simon (1960), which consists of three phases: Intelligence, Design, and Choice. The model has been further extended in the security management literature (Straub and Welke, 1998) to incorporate a total of four phases: the recognition of need or a potential security vulnerability (this corresponds to Intelligence in the Simon model), risk analysis to assess the perceived danger from identified threats, generation of alternative solutions based upon the perceived criticality identified in the analysis (the Design phase), and the planning decision itself is made, with one alternative being chosen out of the possible solutions (the Choice phase).

Figure 1 presents a generalized framework for information system security. The framework follows the general theoretical decision-making model (Simon 1960) and incorporates and extends the three primary categories of managerial perception identified by Straub and Welke (1998). In this framework, security risk planning is given as a process occurring in four phases. First, a security problem or need is recognized (problem formulation and threat determination); second, risk analysis assesses the significance and nature of the identified problem; third, alternative solutions are generated based on perceived criticality; fourth, the planning decision is made (one alternative among identified possibilities is selected).

According to Straub and Welke (1998), the managerial decision making process is influenced by the managerial perception of security, which in turn depends on knowledge of the global environment, knowledge of effective controls, and knowledge of the current environment.

Knowledge of Global Environment includes knowledge of threats and vulnerabilities. Primary sources of information about the global security environment: the mass media, specialist "watchdog" organizations like CERT, and communication through formal and informal channels, within the organization itself. Managerial knowledge, organizational learning through security awareness training and external sources of knowledge (consultants, technology-focused expert systems for operational decision support) comprise the organizational Knowledge of Effective Controls. Knowledge of Current Environment includes identified assets and implemented controls as well as architectural details of the organizational information system. Incorporated with those, the "Operational Security Environment" represents the current overall security posture of the information system by defining acceptable levels of security and then locating the current status within that continuum (von Solms et al., 1994). It serves as a generalized status indicator which should be at the forefront of managerial attention if it should fall beyond a certain threshold.

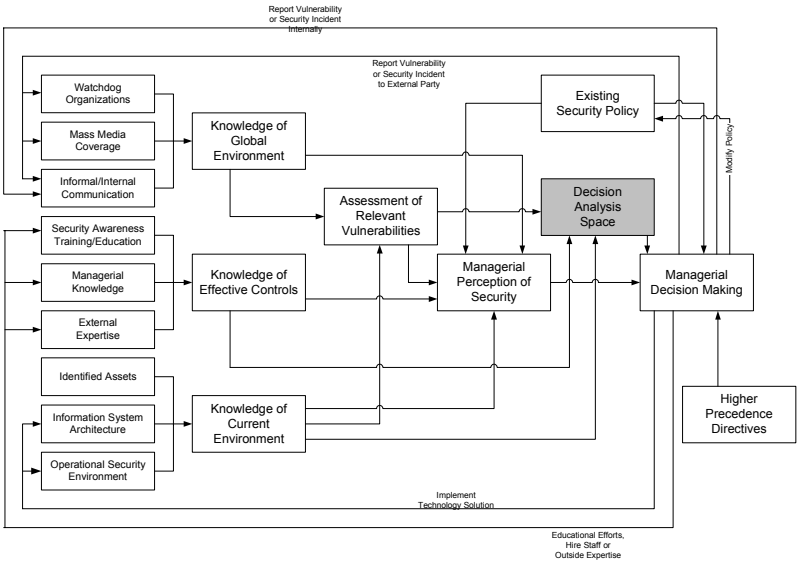

Figure 1. A decision support framework for information systems security

Besides managerial perception, the decision process depends on a definition of the decision analysis space in terms of alternatives and criteria against which these alternatives are evaluated. In addition, the decision process needs to capture the preference structure of the stakeholders toward the identified criteria and alternatives. Finally, the feedback effect of the decision process itself is incorporated, showing the iterative nature of the perceptual model, as it would be used in practice, and how decisions will in turn affect the environment from which future perceptions are drawn.

The model of the decision analysis space

The dimensions comprising the security model are the elements of the security triplet – asset, threat, and control. Identifying sets of these basic dimensions is the first step in formulating an analysis space – eliciting concerns of the problem domain from stakeholders. We can express a list of identified assets, threats and controls as a set of vectors: $V_A = \{A_1, A_2, \ldots, A_n, \ldots, A_N\}$, $V_T = \{T_1, T_2, \ldots, T_m, \ldots, T_M\}$, and $V_C = \{C_1, C_2, \ldots, C_r, \ldots, C_R\}$, respectively. The elements (assets, threats and controls) of each vector are the distinct elements that have been elicited from stakeholders and pertain to the decision situation under consideration. We can characterize each asset, threat, and control element as the vectors:

$A_n = \{P_{A1}, \ldots, P_{As}, \ldots, P_{AS}\}$, where P_{As} denotes the s^{th} attribute associated with element A_s.

$T_m = \{P_{T1}, \ldots, P_{Tu}, \ldots, P_{TU}\}$, where P_{Tu} denotes the u^{th} attribute associated with element T_m.

$C_r = \{P_{C1}, \ldots, P_{Cv}, \ldots, P_{CV}\}$, where P_{Cv} denotes the v^{th} attribute associated with element C_r.

At this level (hereafter referred to as level 1), the decision space is comprised of three sub-spaces, namely, an asset space, a threat space, and a control space. Each decision sub-space can then be described using a set of matrices that capture the evaluation of each element (asset, threat, or control) with respect to the corresponding attributes as well as the preference structure towards the various attributes. Since our space allows for the representation of many simultaneous attributes, we can treat the simple prioritization of assets, threats, and controls as a special case of an MCDM model. For example, regarding assets, we can visualize the corresponding decision space as shown in Figure 2 where we have a number of assets, e.g., customer information, software, etc. that are evaluated and prioritized against a number of attributes such as replacement cost, replacement time, criticality, etc.

Next, we can build a representation space for analysis of comparisons between elements, corresponding to their interactions with one another (hereafter referred to as level 2). We can fully describe this part of the analysis space in terms of three sub-spaces, namely, threats versus assets ($M_{TA} = V_T \times V_A$), threats versus controls ($M_{TC} = V_T \times V_C$), and assets versus controls ($M_{TA} = V_T \times V_A$). Similar to level 1, each decision sub-space also includes a set of attributes as shown in Figure 3 for the 'Risk' attribute. For example, elements for asset-threat combinations may include elements such as "Customer data-Virus attack", while attributes in this decision sub-space may include quantitative risk, defined formally in the classical risk analysis as the product of the cost or loss attributed to an exposure and the probability of an exposure (Courtney, 1977), along

with a qualitative assessment of perceived risk. Accordingly, at this level, MCDM techniques allow the decision maker to rank and prioritize various asset-threat, threat-control, and asset-control combinations against their respective attributes.

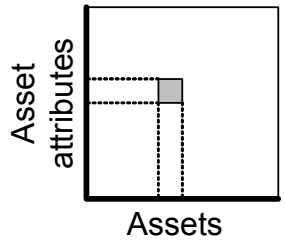

Figure 2. Asset decision sub-space

Taking asset-threat-control combinations we can define an additional decision sub-space (hereafter referred to as level 3), thereby capturing three dimensional decision attributes. Examples of such attributes include effectiveness of a particular control in protecting an asset against a specific threat, and performance impact to an asset by imposing a specific control upon a specific threat.

Using the Model

To use the model, we require first a set of basic elements: assets, threats, and controls. This first stage is preparatory, as it defines the alternatives which are the subject of the inquiry, which will be evaluated against one another. Baskerville (1993) refers to this aspect as a "first generation" security method: the study of the entire repertoire of elements available for a system. We then associate each of these elements with a set of distinct attribute criteria, common between each elemental type but distinct from one another. Thus each asset A_q is associated with a distinct set of attribute criteria (A_qc_1, A_qc_2, … A_qc_m), each threat T_r with criteria (T_rc_1, T_rc_2, … T_rc_n) and each control C_s with (C_sc_1, C_sc_2, … C_sc_p).

The first improvement offered by the explicit representation of the decision sub-spaces consists of the incorporation of multiple-criteria decision-making (MCDM) as an implicit part of preference capturing. This extends the utility of such a tool, elevating security decision-making from what the literature identifies as crude cost/benefit techniques and increasing its flexibility. But again, utilizing the model solely in this way fails to take advantage of the potentially iterative nature of organizational knowledge collection, and it does not directly serve to aid in bridging the managerial/technical gap.

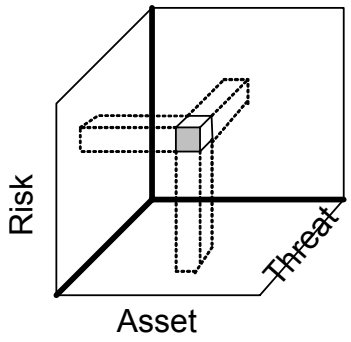

Figure 3. Asset-threat decision sub-space (shown for 'Risk' as a representative attribute)

Expanded use of the proposed framework begins with the eliciting of stakeholder concerns, through providing a list of potential issues, polling opinion or collecting input directly, or through a combination of such methods. These concerns are captured by the system, and then can be prioritized and categorized. In a group decision support setting, we can use a simple or weighted average, or construct a hierarchy, to accurately represent these concerns in accord with the significance of individual inputs to the whole organization. This is conceived to be an iterative process of refinement, and if used as such, cross-functional dialog can be greatly facilitated. Comparison of alternatives within each of the identified dimensions of the analysis space can then occur. This process gradually builds a knowledge base of elemental "facts" upon which the analysis space will draw, and fills in the elements of that analysis space.

Second, the analysis proper must take place. By narrowing the analysis space to elements of interest, a holistic picture emerges from the raw data. The utility of the model lies in its modular nature: taking the basic dimensions of threats, controls, and assets, we can narrow each dimension to include only those items exhibiting characteristics that interest us, and thus simplify the problem domain in terms of this solution space. Relevant criteria entering into the decision are determined, and we progress to alternatives generation after comparison is made for each criterion and preferences are captured within the problem domain. Moreover, the preferences thus elicited are stored for future use by their association with a specific element (threat, asset, control) and their various combinations, within the decision analysis space.

CASE STUDY

The purpose of the case study is to demonstrate the utility of the framework, first as a tool which facilitates balanced managerial perception, and second, as an aid to decision-making. We chose to use the Analytic Hierarchy Process (AHP) (as a representative MCDM methodology) to implement two models which would explicitly capture stakeholder preferences. We briefly explain the basics of the methodology and then proceed to a demonstration, based in part upon a consultation with the Vice President of Technology and managing security officer of a major financial services firm.

AHP, defined in Saaty (1980), is a technique for evaluating and ranking a finite number of alternatives with respect to a number of criteria (decision attributes). The Analytical Hierarchy Process (AHP), as developed by Saaty (1980), is a particularly attractive candidate and representative pair-wise comparison MCDM method which is appropriate to our identified purposes. AHP has been widely applied to a large variety of problems in economics and business operations (Saaty, 1982) as well as information systems, in the existing literature, and has an extensive history of use. Its primary advantage is the ease of making relative comparisons for the stakeholder in an intuitive way, the ability to capture qualitative as well as quantitative evaluations for the various alternatives, the compatibility with group decision making techniques, and the ability to account for dynamic creation of hierarchy levels to any desired level of granularity.

AHP provides for a quantitative pair-wise comparison of alternatives. The process then uses the eigenvalues and eigenvectors of the resulting comparison matrices. The resulting comparison matrices are each associated with a particular three-valued tuple in our analysis space, relative to a particular problem domain for which an AHP model is constructed. AHP naturally leads itself to the types of analysis that can be incorporated in the analysis space we have defined.

The following sub-sections describe each of the models, the results, and the feedback obtained from the aforementioned executives.

Model #1

The model. As shown in Figure 4, the goal for this particular model formulation is to select a security control. At the first level of the hierarchy is a list of relevant assets, which server as the decision criteria in the AHP model. Pairwise comparing these assets against the goal captures the decision maker's perception towards the importance of these assets. In other words, prioritize the assets according to the overall perception of the decision maker. The next level in the hierarchy denotes the threats pertinent to each asset. By pairwise comparing each group of threats against their respective asset, the model captures the decision maker's perception regarding the importance of each threat against each asset. Such perception may implicitly include perception of severity, risk, and exposure (vulnerability). The lowest level (not shown in Figure 4) lists the specific controls (shown in Figure 5) considered in this model. We used the controls identified through the survey conducted in Whitman (2003). We added additional controls relevant to the particular organization in the course of our discussions, and fit them within this same framework.

Results and discussion. Given the preference structure of the decision maker, customer information and data center security ranked highest in terms of importance. Moreover, for customer information, threat to confidentiality was perceived as of highest importance followed by threats to integrity and availability. Again, we can see that these are qualitative threat issues, which could furthermore be broken down into greater detail. For software, acts of human error ranked highest, while for data center security, power outage was perceive as the most important.

Synthesizing the preferences and control evaluations regarding the criteria, 'media backup' and 'no outside connections' ranked highest. The results were consistent with the decision maker's expectation, particularly with the decision maker's emphasis on customer information. Moreover, through sensitivity analysis, the decision maker can visualize how changes in their perception regarding the relative importance of assets, or the relative importance of a particular threat on a particular asset can change the recommended decision. Figure 6 shows how each control ranks in terms of how it is perceived to protect the assets under consideration. The vertical bars denote the relative importance of the assets. By dynamically manipulating the priorities, the rank of the control may or may not change depending on the sensitivity of the results to the relative

importance of the assets. Figure 6b shows the results as the importance of software is increased. In this case, 'employee education' is the top ranked alternative.

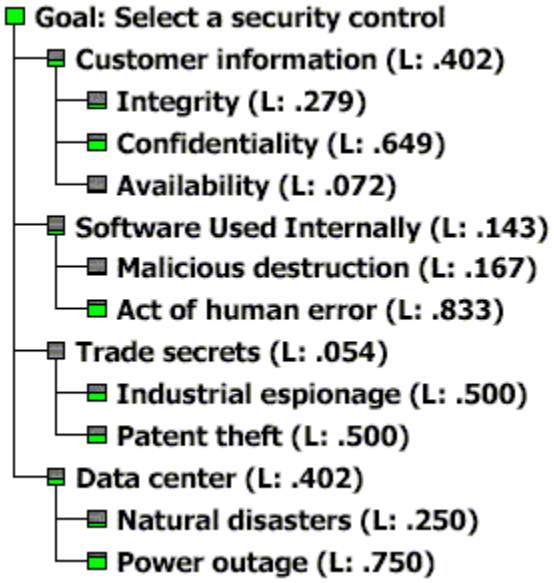

Figure 4. Model #1 hierarchy and ranking.

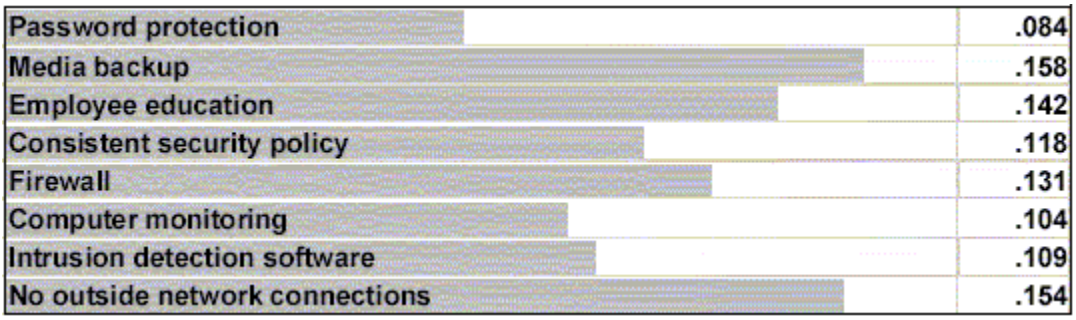

Figure 5. Model #1 ranking of alternatives.

Model #2

The model. Similar to model #1, the goal of this model is the selection of appropriate security controls. However, model #2 presents a different perspective of the decision space. As shown in Figure 7, the first level of the decision hierarchy lists the decision criteria considered when selecting among multiple controls. By explicitly capturing the potential conflict between the cost of the controls and the desired risk exposure, the decision maker can gain a better understanding of the inherent trade-offs among the controls under consideration. Regarding 'risk', the model captures the decision maker's perceptions regarding the risks of various asset-threat combinations. It is worth noting that while the input from the decision maker may reflect the results of a detailed quantitative risk assessment of asset-threat combinations, such assessment may not be required due to the qualitative nature of the inputs required by the model.

Results and discussion. Given the preference structure of the decision maker, 'risk' ranked at a higher priority over 'cost'. Moreover, regarding 'risk', the risk of compromising the confidentiality of customer information ranked highest followed by the risk of disrupting the availability of customer information as shown in Figure 7. Again, we can see that qualitative threats can be incorporated along with physical, quantifiable threats Synthesizing the preferences and control evaluations regarding the criteria, 'intrusion detection' and 'Firewall' ranked highest as shown in Figure 8. The results were consistent with the decision maker's expectation, particularly, with the decision maker's emphasis on the risk exposure for customer information confidentiality and availability, given the nature of the business. Similar to model #1, sensitivity analysis allows the decision maker to visualize the trade-offs involved at any level of the hierarchy, e.g., cost-risk trade-offs and trade-offs among various asset-threat pairs with respect to risk exposure.

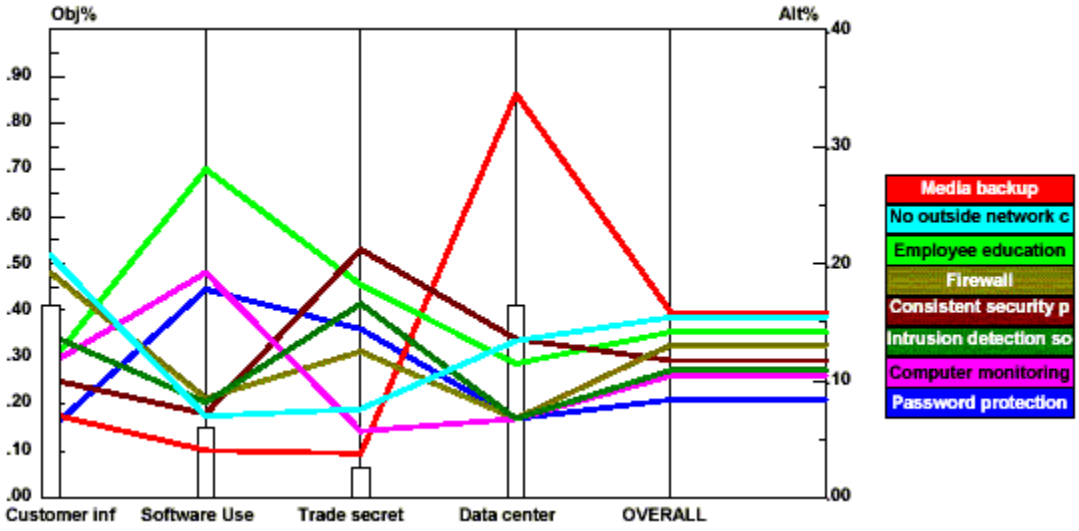

Figure 6a. Model #1 sensitivity analysis – Base scenario.

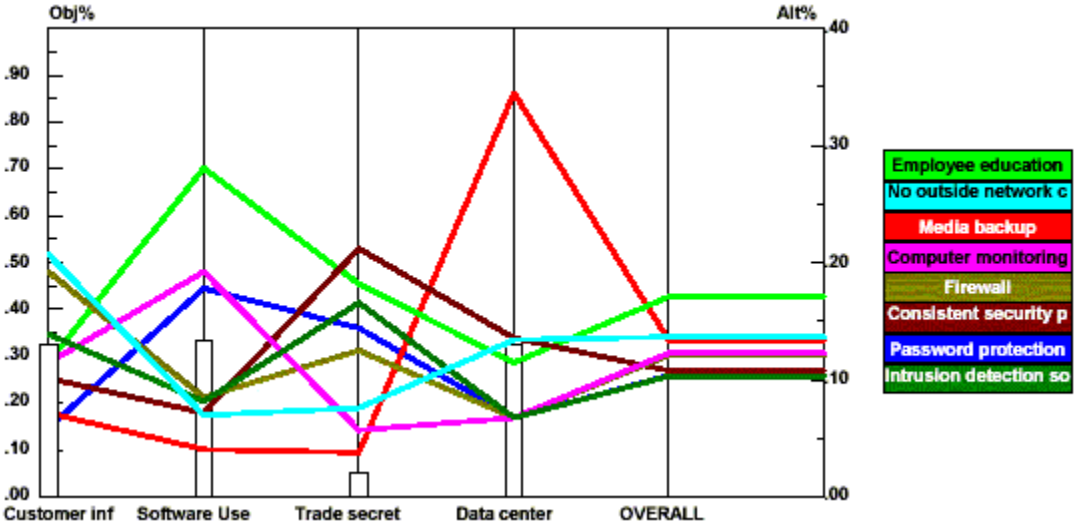

Figure 6b. Model #1 sensitivity analysis – Alternate scenario.

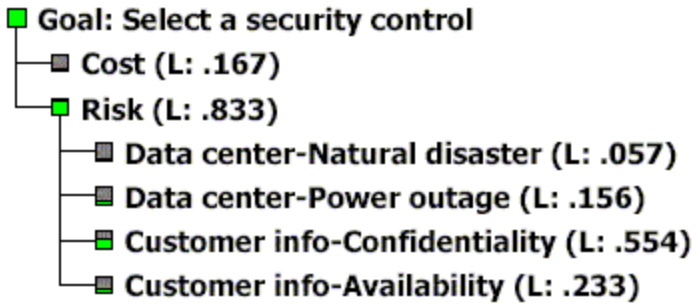

Figure 7. Model #2 hierarchy and ranking.

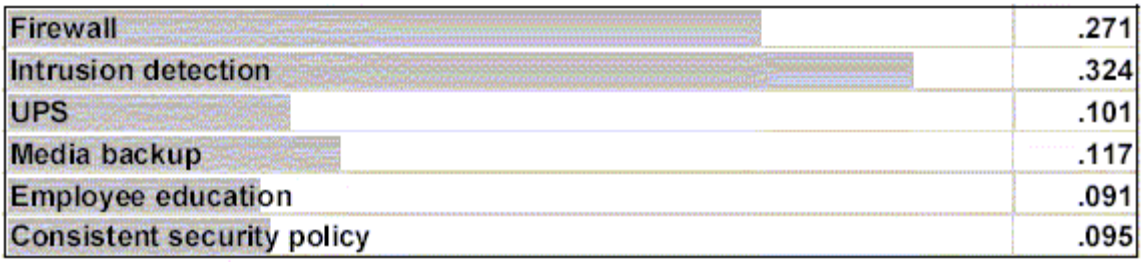

Figure 8. Model #2 ranking of alternatives.

CONCLUSION

As security becomes increasingly relevant in business as well as daily life, and we are gradually ensconced in a ubiquitous sea of information technology, the need for effective security planning, design, and management methodologies and intellectual tools is becoming more important than ever. Nevertheless, existing methodologies and tools for security planning and design are often plagued by a number of issues. Examples of such issues include the inability to capture the multitude of factors involved in security decision making, the difficulty in monetizing values and assets needed for quantitative risk analysis methodologies, the difficulty of capturing perceptions of the various stakeholders, and the ever widening gap among the perceptions of various stakeholders.

Within this paper, we suggest that the incorporation of multi-criteria decision making techniques into information systems security planning and design can make a significant contribution towards improving this situation. The ability to directly represent multiple attributes of the basic security elements through the conceptual tool of a multidimensional decision analysis space is a useful idea in achieving this purpose. The possibility of involving multiple levels of the organization in the decision process, eliciting the preferences, knowledge and expertise cross-departmentally, is in our opinion worthy of significant future research. Decision support can serve as both a tool for facilitating correct perception and as an aid to the decision-making process itself.

The case study involving members from a major financial service provider only served to strengthen our perceptions. They clearly identified issues of business concern to them which could not be easily dealt with: the ability to provide top management with clear and non-technical justifications for issues in security policy and decision and the disconnection which exists between top management's perception of organizational security and the institutional reality.

Of course, this is not to suggest security decision support can become a panacea, but rather to advance the hypothesis that MCDM techniques, which have already been applied successfully to a variety of domains related to social and policy issues, could make a valuable contribution to enhancing the existing information security literature as well as possessing a positive organizational impact.

Further work related to the issues advanced herein will examine the applicability of a variety of multi-criteria techniques, particularly with respect to group decision making. The conceptual tool of a decision analysis space for security, which has been roughly defined within this paper, can be further expanded upon in both representative and judgmental contexts. From a practitioner's perspective, the proposed framework and model for the decision analysis space can form the basis of a new generation of security planning and design tools.

REFERENCES

1. Bandyopadhyay, K., Mykytyn, P. P. and Mykytyn, K. (1999) A framework for integrated risk management in information technology, *Management Decision,* **37,** 437.

2. Baskerville, R. (1993) Information systems security design methods: Implications for information systems development, *ACM Computing Surveys,* **25,** 375.

3. Baskerville, R. and Siponen, M. T. (2001) An Information Security Meta-policy for Emergent Organizations, *Journal of Logistic Information Management*.

4. Courtney, R. (1977) Security risk assessment in electronic data processing, AFIPS Conference Proceedings of the National Computer Conference, Arlington, VA.

5. Dhillon, G. and Backhouse, J. (2000) Information system security management in the new millennium, *Communications of the ACM,* **43,** 125.

6. Ferris, J. M. (1994) Using standards as a security policy tool, *StandardView,* **2,** 72-77.

7. Gregory, R. and Keeney, R. L. (1994) Creating policy alternatives using stakeholder values, *Management Science,* **40,** 1035-1048.

8. Hoffman, L. J. (1989) Risk Analysis and Computer Security: Towards a Theory at Last, *Computers and Security,* **8,** 23-24.

9. March, J. G. and Shapira, Z. (1987) Managerial Perspectives on Risk and Risk Taking, *Management Science,* **33,** 1404.

10. Power R. (2002) CSI/FBI Computer Crime and Security Survey, *Computer Security Issues and Trends,* **8,** 1-24.

11. Raiffa, H. (1982) *The Art and Science of Negotiation,* Harvard University Press, Cambridge, MA.

12. Rees, J., Bandyopadhyay, S. and Spafford, E. H. (2003) PFIRES: A policy framework for information security, *Association for Computing Machinery. Communications of the ACM,* **46,** 101.

13. Saaty, T. L. (1980) *The Analytic Hierarchy Process,* McGraw-Hill, New York.

14. Saaty, T. L. (1982). Decision making for leaders. Belmont, CA: Lifetime Learning Publications division of Wadsworth, Inc.

15. Straub, D. W. and Welke, R. J. (1998) Coping with systems risk: Security planning models for management decision making, *MIS Quarterly,* **22,** 441.

16. Thomas, H. and Samson, D. (1986) Subjective Aspects of the Art of Decision Analysis: Exploring the Role of Decision Analysis in Decision Structuring, Decision Support and Policy Dialogu3e, *Operational Research Society,* **37,** 249-265.

17. Von Neumann and Morgenstern (1944). Theory of Games and Economic Behavior. Princeton, NJ: Princeton University Press.

18. von Solms, R., van de Haar, H., von Solms, S. H. and Caelli, W. J. (1994) A framework for information security evaluation, *Information & Management,* **26,** 143.

19. Whitman, M. E. (2003) Enemy at the gate: Threats to information security, *Association for Computing Machinery. Communications of the ACM,* **46,** 91.

20. Willison, R. and Backhouse, J. (2003) Understanding Criminal Opportunity in the IS Context, IRIS, Finland.