2010

A web-based multi-perspective decision support system for information security planning

Omar F. El-Gayar
Dakota State University

Brian D. Fritz
Dakota State University

Recommended Citation

El-Gayar, O. F., & Fritz, B. D. (2010). A web-based multi-perspective decision support system for information security planning. Decision Support Systems, 50(1), 43-54.

Decision Support Systems 50 (2010) 43–54

Contents lists available at ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss

A web-based multi-perspective decision support system for information security planning

Omar F. El-Gayar [a,*], Brian D. Fritz [b]

[a] Dakota State University, 820 N. Washington Ave., Madison, SD 57042, United States
[b] Dakota State University, United States

ARTICLE INFO

Article history:
Received 30 June 2008
Received in revised form 27 April 2009
Accepted 11 July 2010
Available online 27 July 2010

Keywords:
Information systems security planning
Decision support
Multiple criteria decision making
Inquiring organizations

ABSTRACT

With the increasing exposure and vulnerability to cyber attacks, it becomes necessary to develop methodologies and systems that are capable of dealing with the complex and multifaceted nature of decision situations encountered in security planning and management. In this paper we present the theoretical basis, architecture and design of a web-based multi-perspective decision support system (DSS) and an underlying decision multi-criteria decision framework that is consistent with security and decision theory. The system is illustrated through a multi-stakeholder scenario that captures the complexity encountered in a multi-criteria security control selection decision problem.

1. Introduction

In today's competitive and dynamic business environment, organizations are increasingly reliant on information technology for increased efficiency and for securing competitive advantage. Unfortunately, with the ubiquity of information technology (IT) comes increased exposure and vulnerability to cyber attacks. According to the Computer Security Institute (CSI), the average annual loss reported in their 2008 survey is $289.6 thousand, down from $345 thousand last year, but up from $168.7 thousand two years ago [46]. Earlier reports also present a similar picture. PricewaterhouseCoopers L.L.P. and InformationWeek reported an estimated $1.6 trillion dollars in damage on the global economy and $266 billion within the United States [7]. While the surveys mentioned may provide varying statistics due to the diverse populations (different countries, sectors and degree of sophistication about security matters) [43], such numbers convey to us a clear signal that security remains a continually significant issue with growing organizational as well as economic impacts.

Despite the proliferation of IS security risk analysis methods the data needed for decision making is not known with any accuracy and it is thus not clear how organizations make security investment decisions [43]. More importantly, such risk management approaches acknowledge that "risk perception depends very much on beliefs, feelings and judgment" [17]. Tools and methods for security risk planning which rely on techniques that ignore behavioral aspects cannot account for the multidimensional effects of security controls [57]. Moreover, the security literature and practice has in the past decade come under wide criticism from the socio-technical research community, as being largely technocratic e.g., [64] and functionalistic in its approach to information security, at the expense of the organizational aspect [26]. The multidimensional nature of security awareness [53] precludes, from this perspective, the ability of traditional security management approaches to consider significant factors that are not easily quantifiable within their decision making, and would seem to extend the traditional scope represented best by the so-called "C.I.A." paradigm of Confidentiality, Integrity, Availability [21].

If we are to consider information security as a holistic and organizational concern, it follows logically that our methods of management must be able to accommodate this vision. Organizations which exhibit higher levels of inquiry [8] require tools appropriate to their level of decision making. Following Courtney [9], decision support systems must embrace approaches that respond to the decision styles and complexity exhibited in such organizations. Moreover, multi-criteria decision making (MCDM) accompanied by group decision support (GDSS) techniques can meet such requirements and thus improve the security decision process in these organizations.

Within this paper, we develop a collaborative web-based decision support system (DSS) for security decision making and planning, incorporating notions drawn from inquiring systems, multi-criteria decision analysis and group decision making. The Analytic Hierarchy Process (AHP) is incorporated into a distributed web application for decision support, and an example of its use in addressing a security decision problem is given. The remainder of the paper is organized as

* Corresponding author.
E-mail address: Omar.el-gayar@dsu.edu (O.F. El-Gayar).

0167-9236/$ – see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.dss.2010.07.001

follows: the next section provides a brief review of relevant literature. We then present the design and development of the system and follow with a multi-stakeholder a multi-criteria scenario demonstrating the applicability of the proposed system. We conclude the paper with reflections and direction for future research.

2. Literature review

2.1. Security planning decision making

Quantitative and mathematical analysis approaches to security investment and management have been heavily emphasized, e.g., [5,20,28], largely from a fiscal, cost-containment perspective. Many of these techniques draw directly from financial management and risk management. Examples of such techniques are: Return on Security Investment (ROSI), common financial measures such as Net Present Value (NPV) and Internal Rate of Return (IRR) for evaluation of a potential security investment, and risk management approaches based on expected value, an example being Annualized Loss Expectancy.

These methods are all constrained by the difficulty in quantifying the probability of a threat to an IS asset, the value of assets, and the related ISS risk [19,59]. Recent contributions to the security planning literature have acknowledged such difficulty [7,44,49,59] and have attempted to provide alternative approaches that reduce the demands on the data requirements [7,15]. Others have emphasized the importance that accurate estimation of system risk plays in the success of risk management [65], yet the analytic models provided do not offer specific guidelines for obtaining the necessary data. Regardless of the approach, the data requirements for analysis continue to prove an extremely difficult task [19,29,33] particularly as the nature of today's information technology and business environment emphasizes securing information and intangible assets which in turn can prove a far more daunting task than quantifying the value of physical assets.

There have also been substantial arguments for subjective behavioral approaches. Behavioral security research suggests that in practice, probability estimates tend to be underemphasized in importance relative to worst-case scenario [31]. This research recognizes the role of managerial perception and subjective criteria (beliefs, feelings, judgments) as major influences on risk tolerance in information security [40,57,58]. It purports that techniques which ignore behavioral aspects cannot account for the multidimensional effects of controls [57] and are often atheoretical [23]. Additional problems include issues of communication between management tiers as discussed in [3], often resulting in inconsistency and reactive policy [18].

There exists a need for approaches and systems that address decision-making needs in complex situations, such as security planning, that involve multiple perspectives [12,19,66] and are frequently plagued by inadequate data and multiple, often conflicting, goals. Problems encountered in this context are often referred to within the literature as "wicked" problems [48] and exhibit troublesome characteristics, including the following significant issues:

- There is no definite formulation of a wicked problem — formulating the problem is the problem.
- Solutions to wicked problems are not necessarily true or false, but good or bad — values are inherently a large part of the problem and the values employed vary among stakeholders.
- There is no immediate or ultimate test of a solution to a wicked problem.
- Every solution to a wicked problem is a "one shot operation"; because there is no opportunity to learn by trial and error, thus every attempt counts significantly.

In attempting to deal with such "wicked" decision situations, any proposed system should embrace a Singerian organizational model for inquiring organizations [9] that goes beyond the technical and reductionistic orientation of most existing approaches. MCDM is purported as a means for handling goal imprecision and conflict often encountered in such situations, as we shall elaborate.

2.2. Security planning in inquiring organizations

Churchman's [8] seminal work on inquiring organizations as learning organizations provides us with a comprehensive framework for defining intelligence in systems, and thus, for valid approaches to handling complex problems like those encountered in security planning. The characteristic decision making for these organizations may vary depending on their underlying epistemology (or philosophy of knowledge) [9]. For example, while a normative Leibnizian (rational) inquiring organization views itself as creating knowledge by using mathematical analysis and formal logic to make inferences about cause-and-effect, a Lockean (empirical objectivity) inquiring organization creates knowledge through observation, and sharing and creating consensus about these observations. With respect to decision styles, Leibnizian organizations are analytic in nature, wherein the world can be reduced to formulas and assumptions, while a Lockean organization emphasizes a more open and group-oriented approach to decision making under a similar reductionist paradigm. It should be noted that most approaches to decision support in the context of security planning have been oriented towards such organizations and assume a paradigm characteristic of such "old thinking" [34].

At a higher level of inquiry as it is identified by Churchman, Hegelian (dialectical or conflict-based) and Kantian (multi-perspective) inquiring organizations may exhibit "complex thinking" decision styles [34]. In a Hegelian organization, knowledge is created by observing a conflict manifested as a debate between two diametrically opposed viewpoints about a decision situation. Such debate may reflect more than one perspective on the decision problem and has been found as an effective approach to surfacing assumptions in strategic planning problems [32]. Groupware and negotiation support systems have been found to be well suited for this approach [9]. A Kantian inquiring organization would also recognize that there may be multiple valid perspectives from which to view and model a problem, not necessarily in the context of a conflict. The decision style in such organizations emphasizes the development of multiple interpretations of data by relying heavily on analytical methods [9].

Mitroff and Linstone [34] go a step further by advocating a "new thinking" as exhibited in Singerian organizations. In such organizations, the "world" is viewed as a holistic system. Problems must be analyzed as a whole, capturing multiple perspectives in their thinking and decision making [9,30,34]. In capturing multiple perspectives, Singerian organizations surpass the other forms of inquiring organizations reflecting only a technical (T) perspective, in effect using any and all forms of inquiry whenever and wherever appropriate in the decision making process [9]. Such technical perspective is thus augmented by organizational/social (O) and personal/individual (P) perspectives [34].

We find these higher modes of inquiry necessary to a socio-technical system for decision support as useful approaches to issues which are peculiarly complex, in that their analysis may require the consideration of ill-defined problems, heterogeneity of levels of communication. Highly context-dependent concerns exist where objectivity is difficult or impossible, and must rely on subjective judgment (at and above the "Kantian" mode of inquiry) and thus on *a posteriori* as well as *a priori* reasoning. To extend the organizational system to higher modes of inquiry requires additionally the establishment of organizational memory [55] by supporting the collection and aggregation of individual knowledge that is collaboratively accepted, [47] and facilitating its timely recall by some

associative process. The facilitation of organizational learning [51] requires not merely that existing knowledge, in the form of conceptual schemas and scenarios, be available, but that such knowledge actively supports future actions, and thus aids future decision making.

2.3. MCDM and group decision support

The security decision process as we would define it consists of a process 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 made is able to achieve the objective of the decision. Security decisions made in the presence of multiple, and often conflicting, criteria (both qualitative and quantitative) on the basis of multiple stakeholder inputs require the use of methods suitable to multiple criteria decision making (MCDM). Moreover, MCDM would seem a natural technique to support the sort of organizational learning through group collaboration (see [36]) identified above. According to Stewart [56] (p. 569), "the key philosophical departure point defining Multiple criteria decision making (MCDM) as a formal approach to types of problem solving (or mess reduction), lies in attempting to represent such imprecise goals in terms of a number of individual (relatively precise but possibly conflicting) criteria". In effect, MCDM techniques are particularly suited to complex decision situations involving imprecise and often conflicting goals.

Multi-attribute utility theories (MAUT) utilize this notion explicitly in the decision process [37]. Utility-based MCDM techniques imply the existence of a utility function, a statement of an objective value that can be maximized and objectively measured. Unfortunately, this "utility function" has proved to be extremely elusive except in the simplest problems [39], particularly for multi-objective questions. Practically, we note further consequences in terms of the expected capability of organizations to utilize such methods. These techniques entail expert knowledge of objective phenomena. Moreover, the inability to represent qualitative attributes limits greatly the preferences we can capture.

Qualitative MCDM techniques would seem to offer us greater possibilities in addressing these concerns. Their advantage lies in the ability to rank alternatives relative to one another, without a need for objective measures [16]. The Analytical Hierarchy Process (AHP), developed by Thomas Saaty [50], is an MCDM method well suited to deal with these issues. AHP has been widely applied to a large variety of problem domains in economics, business operations, and information systems. As a technique, AHP facilitates qualitative comparisons [62] as well as meaningful comparisons given incommensurable unit measures [25] and can also accommodate quantitative data [50]. The explicit use of pair-wise comparisons means that trade-offs in conflicting criteria are made obvious to the decision maker. Compared to other MCDM techniques, AHP is easy to understand [38]. It is simple-to-use, intuitive and the details of implementation and calculation can be hidden without affecting the usability of the results [6,63], and supports creation of decision hierarchies incorporating multiple factors of a decision. Moreover, in addition to supporting the Choice phase of Simon's [52] model of decision making [10], AHP may support the Intelligence and Design phases [2], as well as the Implementation through prioritization of activities encountered in a decision situation [42]. These advantages make AHP a natural choice as the analysis engine, in combination with group support techniques, within the proposed system.

In the context of security planning, Bodin et al. [4] illustrates how AHP can help organizations make an information security investment decision. In this paper, we advance upon that work in meeting the needs of inquiring organizations in multi-perspective decision making by providing a detailed depiction of the decision space at multiple and increasing levels of detail, realized as a series of AHP models explicitly representing the interaction of assets, threats, and controls, and in supporting aggregation of input from multiple stakeholders. Moreover, adaptations of AHP to the support of a group decision making context have been made [10,35,60]. Our approach combines individual subjective judgments expressed as preference structures over a common set of criteria, which we are suggesting to be necessary in supporting the higher levels of inquiry (in particular Kantian, and by extension, Hegelian and Singerian) as characterized above. This is combined with group interaction which may occur before or after the individual (subjective and qualitative) preferences have been elicited and collected.

3. System requirements

In facilitating the design of a decision support system to support higher modes of organizational inquiry, we have identified a number of key attributes which the literature identifies as characteristic of these modes of inquiry. We can now deduce a number of requirements necessary to support these modes of inquiry (Kantian, Hegelian, and Singerian) within the proposed system. This corresponds to activity 2 "Define the objectives for a solution" of the design science research methodology as outlined in [41]. These requirements are:

A) Support multiple stakeholder perspectives (Kantian inquiry) and subjective perceptions.
B) Capture individual judgments which may conflict or cohere (Hegelian inquiry).
C) Incorporate means of aggregating these preferences and evaluating the outcome.
D) Accommodate ill-structured or semi-structured problems requiring open systems and iterative judgments involving multiple and often conflicting criteria.
E) Facilitate 'organizational memory' through the storage and recall of previous judgments.
F) Encourage consensus formation through repeated iterations and compromises.
G) Disseminate approved outcome of the decisions made should be available to support future judgments and scenario creation.

We now present the design and development of the system and the underlying decision model in order to meet the aforementioned requirements.

4. System design and development

4.1. The underlying decision model

The dimensions comprising the security model are comprised of an asset, a threat, and a control dimension. They are defined as follows: **T** is the set of known threats **T**:[t_1, ... , t_n] which may impact a security decision made by the organization. **C** is the set of all known managerial or technical controls, **C**:[c_1, ... , c_m], which might form part of a security decision. Finally **A** is the set of all identified assets **A**:[a_1, ... , a_q] which might be attacked by some set of threats **T**:[t_1,..., t_n], and/or protected by some set of controls **C**:[c_1 , ... , c_m]. Identifying subsets of these basic global dimensions is the first step in formulating an analysis space for eliciting concerns of the problem domain from stakeholders.

For any given problem scenario S, 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 $V_C = [C_1, C_2, \ldots, C_r, \ldots, C_R]$, (where V_A, V_T, V_C, are subsets of **A**, **T**, and **C** respectively). The elements (assets, threats and controls) of each vector, in turn, are the distinct elements that have been elicited from stakeholders and pertain to the decision situation

under consideration. We define each asset (A_n), threat (T_m), and control (C_r) element in terms of attributes:

$A_n = [P_{A1}, \ldots, P_{As}, \ldots, P_{AS}]$, where P_{As} denotes the sth attribute of A_n.
$T_m = [P_{T1}, \ldots, P_{Tu}, \ldots, P_{TU}]$, where P_{Tu} denotes the uth attribute of T_m.
$C_r = [P_{C1}, \ldots, P_{Cv}, \ldots, P_{CV}]$, where P_{Cv} denotes the vth attribute of C_r.

Next, we can build a representation space for analysis of comparisons between elements, corresponding to their interactions with one another. This part of the analysis space is comprised 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 ($M_{AC} = V_A \times V_C$). Each decision sub-space includes its own unique set of attributes. For example, elements for asset–threat combinations may include elements such as "Client information/insider abuse", while attributes in this decision sub-space may include a quantitative risk assessment along with a qualitative assessment of perceived risk or even an attribute representing perceived impact on public image from such an incident. Accordingly, MCDM techniques allow the decision maker to rank and prioritize various asset–threat, threat–control, and asset–control combinations against their respective attributes. Taking asset–threat–control combinations next, we can define an additional decision sub-space to be associated with a set of criteria, thereby capturing three dimensional decision attributes. Examples of such attributes include effectiveness of a particular control in protecting an asset against a specific threat.

Use of this underlying model facilitates thinking about security problems in a manner that is understandable in operational terms, and is capable of producing actionable decisions. However, the implementation of the various levels defined above will be abstracted away from the user by designing the system around a scenario-based approach to simplify and speed up the process of using the system. Efraim et al. [11] recognize the importance of scenarios in management support systems. Most notably, scenarios help identify opportunities and problem areas, provide flexibility in planning, help validate modeling assumptions, and allow the decision maker explore the behavior of the system under various assumptions. Moreover, scenarios can serve as means for capturing organizational memory.

4.2. System architecture

The system is comprised of three major functional areas: scenario maintenance, MCDM analysis engine, and group preference aggregation. This connected set of subsystems provides the modular infrastructure upon which the presentation-level access (i.e., the user interface) is built, and is supported by database for storing various scenarios and supporting decision elements. The following sections briefly describe each of these identified modules.

4.2.1. Scenario maintenance

The system is based upon user creation and ownership of scenarios, which are designed and administrated by the users, who may in turn grant other users access to the scenarios as stakeholders, open scenarios to receive input judgments, examine scenario progress and publish completed scenario results to the group. The scenario maintenance module facilitates scenario creation through the scenario editor (see Fig. 3), in mapping chosen elements and criteria to existing scenarios if possible, and creating unique elements only when necessary. The user is also able to search through the existing base of scenarios for particular elements of interest (see Fig. 2), and can derive a new scenario from an identified scenario if they wish. This serves to limit greatly duplication of elements (one of the earliest problems we faced in experimenting with the framework) and facilitates iterative use of the system through the establishing of association relations, linking scenarios to one another and reusing a common base of related assets, threats and controls, as well as allowing an existing scenario to act as a template for creating a new one. This addresses design requirement "E" in supporting organizational memory and knowledge reuse by preserving and drawing elements from previous scenarios. It also provides basic maintenance functions and allows assignment of users as scenario stakeholders.

This module makes it possible to abstract the decision framework details from the user and thus to simplify the process from the end-user standpoint. Our model for the MCDM decision framework above delineates a series of analysis spaces corresponding to the basic operational security notions of Asset, Threat, and Control and combinations thereof. The scenario maintenance module handles the translation of these elements into the star schema, generating relational links between scenarios and reusing existing combinations held in common between existing scenarios. In addition to abstracting the process details away from the user, this approach facilitates efficiency and element reuse in user scenario design through the association process.

4.2.2. MCDM analysis engine

The MCDM analysis engine must facilitate use of the decision model in a manner which will allow for comparison of alternatives across multiple criteria, the result of which is a prioritized list of alternatives. The initial prototype of the system uses AHP as its inference engine, for reasons discussed earlier. However, the proposed system could be adapted to utilize different MCDM methodologies as well. This module supports system requirements "A" and "B", listed above, in that it is capable of capturing multiple stakeholder perspectives on a shared scenario, and can deal with conflicting criteria through the use of a pair-wise comparison in its preference capturing.

We store the results for both criteria and alternative judgments to allow us to dynamically calculate judgments from the stored priorities from multiple stakeholders who are accessing the system at different times, and to allow for ease of adjustments when performing these aggregations for sensitivity analysis, as well as allowing for future integration with other data sources. Storing these judgments is also necessary in order to support group preference aggregation.

4.2.3. Group preference aggregation

Given the requirements of the system necessary to support the highest levels of organizational inquiry (Hegelian and Singerian), we felt that stakeholder feedback should be the prime element for moving towards a consensus. The stakeholder is able to reject results if he disagrees with the individual result, and repeat the process until the scenario is closed to further input by the scenario owner. The scenario owner is given supervisory access to the scenario after all judgments have been taken, allowing for sensitivity analysis, as he is then able to weight stakeholder judgments dynamically and can in turn see how this affects the final results. He must eventually make the aggregate result available to stakeholders. To this end, the system allows the scenario designer to 'publish' the aggregate result (see Fig. 5) and the stakeholders are then able to vote in support of the final result or to dispute it, possibly even resulting in the scenario owner restarting the scenario from scratch or abandoning it altogether. It should be noted, however, that while consensus is desired (and may be achieved through multiple iterations), it is not guaranteed.

A number of preference aggregations schemes exist in the literature [1,10,45,50,54]. In this system, we use the weighted arithmetic mean method (WAMM) for aggregating individual priorities (AIP). Such method is the only method that satisfies the unanimity condition (Pareto principle) [45], as well as possesses other desirable features such as the homogeneity conditions and the reciprocal property [14]. Regardless of aggregation method, the scenario owner will need to provide individual participants' weights (if they are not to be equally weighted). Such weights may reflect the scenario creator's subjective judgment regarding the experience, expertise, and knowledge of the individual participants.

This module fulfills system design requirement "G" and completes "C" in combination with the Analysis engine, in the ability to produce judgment based on a multiple stakeholder aggregate. It also facilitates requirement "D" and "F" in that the scenario creator can opt to allow users to repeat the judgment process, or can elect to abandon and restart the scenario altogether, and in that it allows users to vote against and thus reject the scenario result if they dispute it.

4.3. Using the system and underlying decision model

Based upon the Simon [52] model of general decision making, and the contribution of Straub and Welke [57] with respect to security management, the overall decision process will be described in terms of four basic phases. First, a security problem or need is recognized (problem/goal formulation, asset prioritization, and threat determination); second, risk analysis assesses the significance and nature of the identified problem (solicitation of stakeholder judgments); third, alternative solutions are generated based on perceived criticality (selection of control); fourth, the decision is carried out (implementation). Accordingly, use of the system begins with defining the decision space and eliciting of stakeholder concerns, through providing a list of potential issues, polling opinion or collecting input directly, or through a combination of such methods. 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. Comparison of alternatives within each of the identified dimensions of the analysis space can then occur, as discussed previously. After stakeholder judgments are taken, they can then be prioritized by the scenario owner. In a group decision support setting, the system aggregates the preferences of the individual stakeholders and presents the information to the scenario owner. The scenario owner may then publish the results for group feedback. This is an iterative process of refinement which encourages the generation of a consensus, to facilitate dialog on the problem area and/or to re-evaluate the scenario (or even serve to spin-off a related new scenario for future analysis). The general procedure for using the system is as follows (Fig. 1):

1. Users examine and can add to the collection of basic elements (assets, threats, and/or controls) that are drawn upon later in designing scenarios.
2. A user interested in creating a scenario uses the searchable knowledge base of archived scenarios, to find previous cases that used similar elements, and may view the accepted results of the archived scenario if they are available.
3. The user may elect to derive his scenario from a previous case that he has located, or may simply begin a new scenario. The system provides a list of previous criteria from scenarios of the same type, or allows creating unique criteria for this instance.
4. The user assigns stakeholders (other users) who are then authorized to access the newly designed scenario and input their preferences to the system.
5. The stakeholder who is making pair-wise judgments is at their conclusion able to view the resulting priorities and may opt to repeat the process if s/he disagrees with the result; otherwise the preference details are recorded to permanent storage.
6. The scenario creator views aggregate judgments and can examine judgment sensitivity by temporarily altering stakeholder weights.
7. The scenario creator completes the scenario, opening the aggregate results to all stakeholders.
8. Stakeholders view the final choice and vote on the final outcome.

5. System demonstration

According to Peffers et al. [41], once the design and development of the system (artifact) is complete, the next step is to demonstrate the use of the artifact to address the problem identified earlier as outlined in Section 3. In this paper, we extend upon earlier work conducted in consultation with a financial services provider that illustrated the viability of an MCDM-based approach. In this demonstration, we use the system to address a complex realistic scenario where multiple model iterations are necessary to solve a problem, namely assessing risk and evaluating relevant countermeasures (controls). The scenario is based on a generic risk assessment process outlined in [27] and highlights the handling of multiple perspectives and qualitative criteria within the framework. In this scenario, a financial firm needs to select and prioritize security controls, and wishes to make the most effective possible choice by incorporating the concerns of several groups of stakeholders, to protect the most valuable assets against the most dangerous threats. We will involve a variety of functional areas in the decision making, with different areas of expertise and agendas, and decompose the problem using a series of models to better manage the complexity of the underlying decision situation.

There are three primary groups of stakeholders: Executives, who will be asked to address survivability concerns and monetize assets, Legal, who will deal with liability issues, and a Technical unit will address IT/networking concerns. The functional groups will use the results of these assessments and priorities developed to make a collaborative control selection decision based on aggregate preferences from each of the representative stakeholders.

Having identified the primary goal of control (countermeasure) selection, we begin our security assessment with asset prioritization by defining the asset sub-space. Since there may already be an inventory of organizational assets (also referred to as an asset registry), the scenario owner (on behalf of the stakeholders) consults the scenario knowledge base, searching for existing asset evaluation scenarios relevant to current security concerns. The scenario of concern evaluates a set of organizational assets in three major asset categories, namely, Information assets: Client information, Intellectual property (a proprietary credit risk model), People: information technology staff and functional area staff, and Physical assets: data center and client desktops/laptops. Following Jones and Ashenden [27], assets are prioritized along the following common criteria:

- Confidentiality: Impact on the organization if the confidentiality of the asset is breached.
- Integrity: What is the impact on the organization if the integrity of the asset is breached?
- Availability: Organizational impact if the availability of the asset is compromised.

The results emphasize Confidentiality and Integrity over Availability and indicate the prevalence of Client information and Data center as the most important assets. A selection of threats is also taken from a comprehensive list given in the latest CSI 2008 survey of computer crime and security [46]. Threats of unauthorized access and insider abuse are identified as the highest priority. Fig. 2 provides a list of available scenarios in the knowledge base.

Following Jones and Ashenden [27] we then proceed to assess the risk of a particular threat to a particular asset. This corresponds to a two-dimensional sub-space of assets and threats. To manage the complexity of the next level of analysis, the scenario owner includes the two highest priority assets: customer information and data center, and the two highest priority threats: insider abuse and unauthorized access, previously identified. Accordingly, this scenario is comprised of four alternatives corresponding to all relevant asset–threat combinations. The criteria included in this scenario are:

- Vulnerability: The security weakness that exposes a particular asset to a particular threat.
- Impact: The cost of the threat compromising the information asset.
- Probability: The likelihood that a particular threat will affect a particular asset.

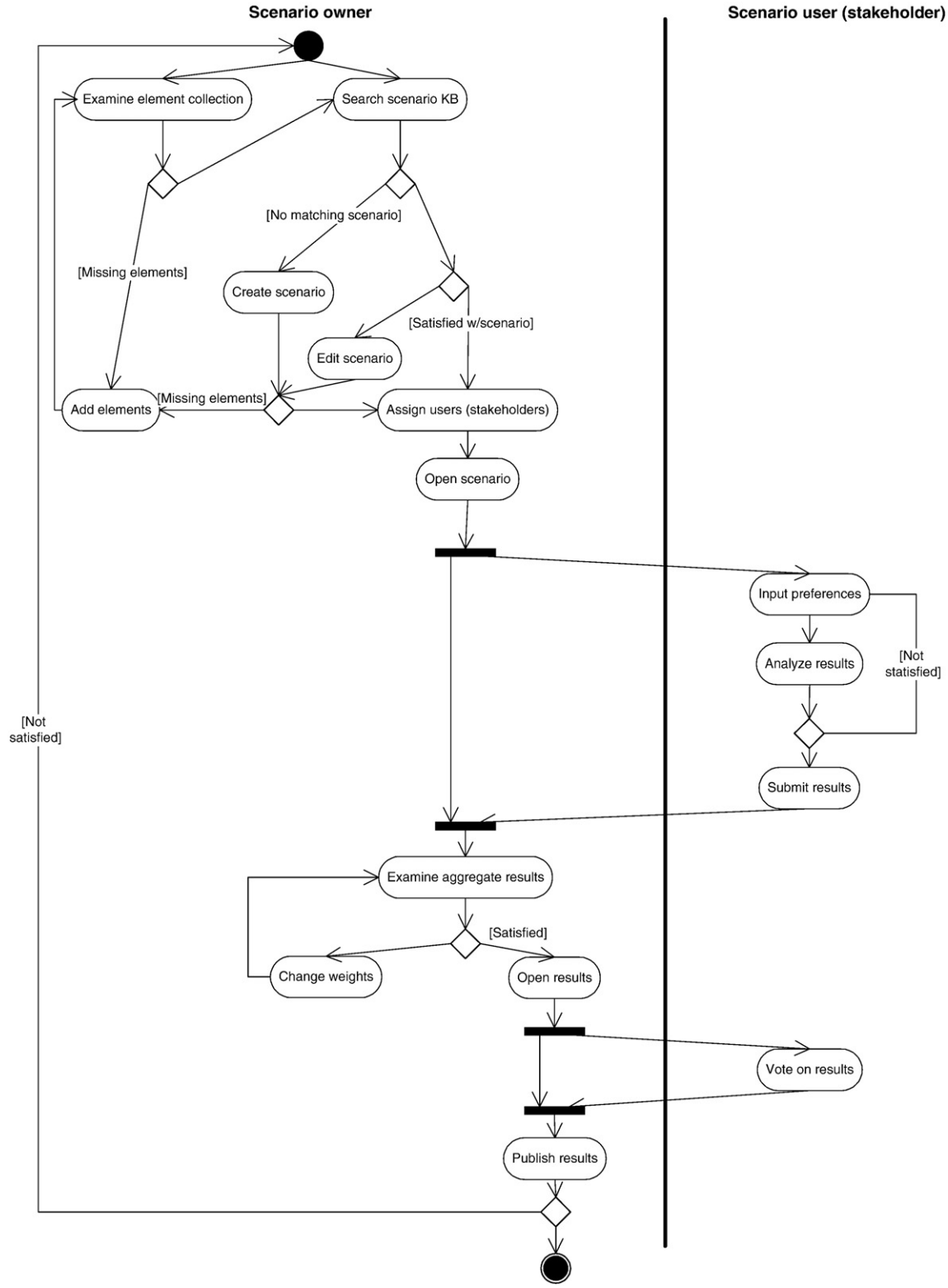


Fig. 1. System flow diagram.

With these assets in mind, the scenario owner breaks down a risk assessment across these two top-priority assets identified in the previous model, resulting in the scenario of Fig. 3. This scenario will be conducted in a decentralized manner allowing for individual inputs of three stakeholder groups, Executive, Legal, and Technical, independent of one another and aggregated to examine consistency and robustness of the decision. We have summarized the remaining results in Table 1. Executives exhibit Impact (the expected loss or cost of compromise) as the dominant criteria (shown in Fig. 4), and Legal views Vulnerability (exposure to threat occurrence) as most significant. Executive and Legal strongly favor "Client information/Insider abuse" by their respective criteria structures, followed by lesser preferences for the two alternatives "Client information/Unauthorized access" (favored by Executive) and "Data center/Unauthorized

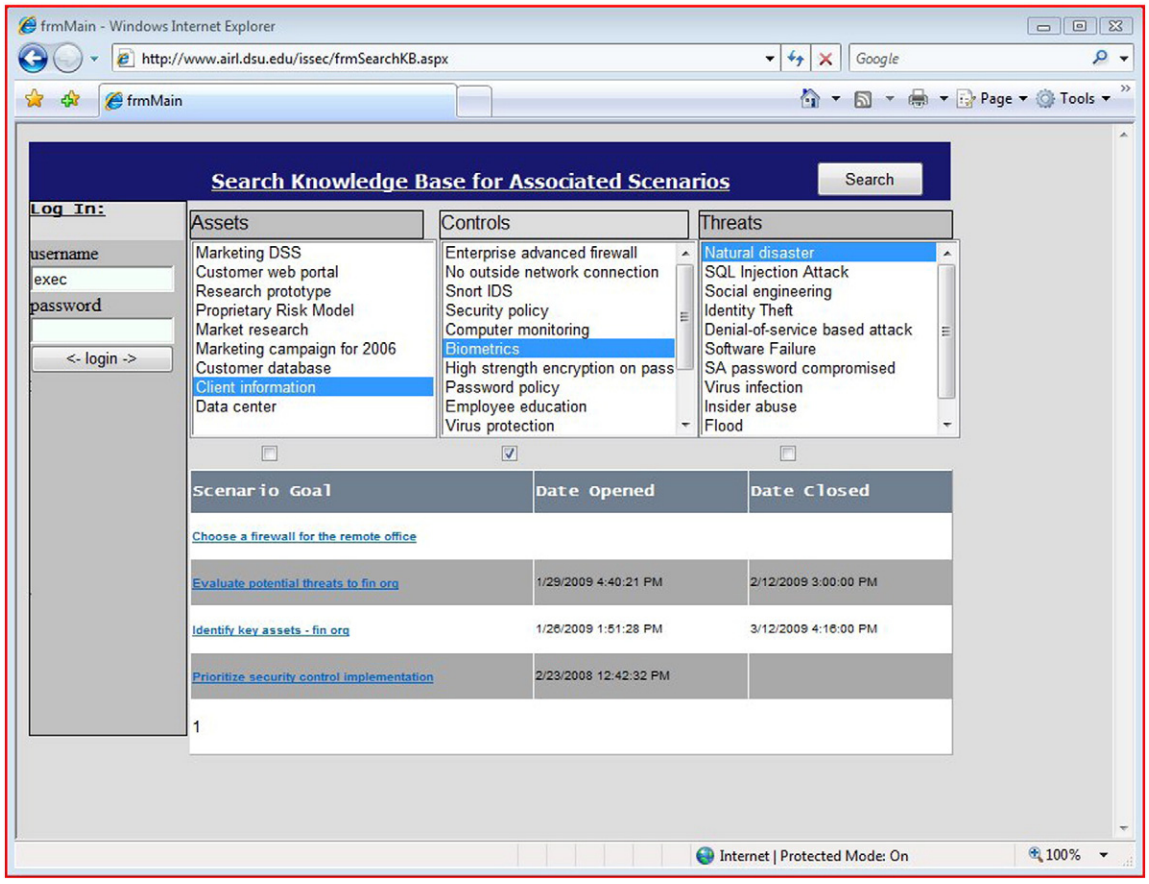


Fig. 2. Searchable database of scenarios, assets, threats and controls.

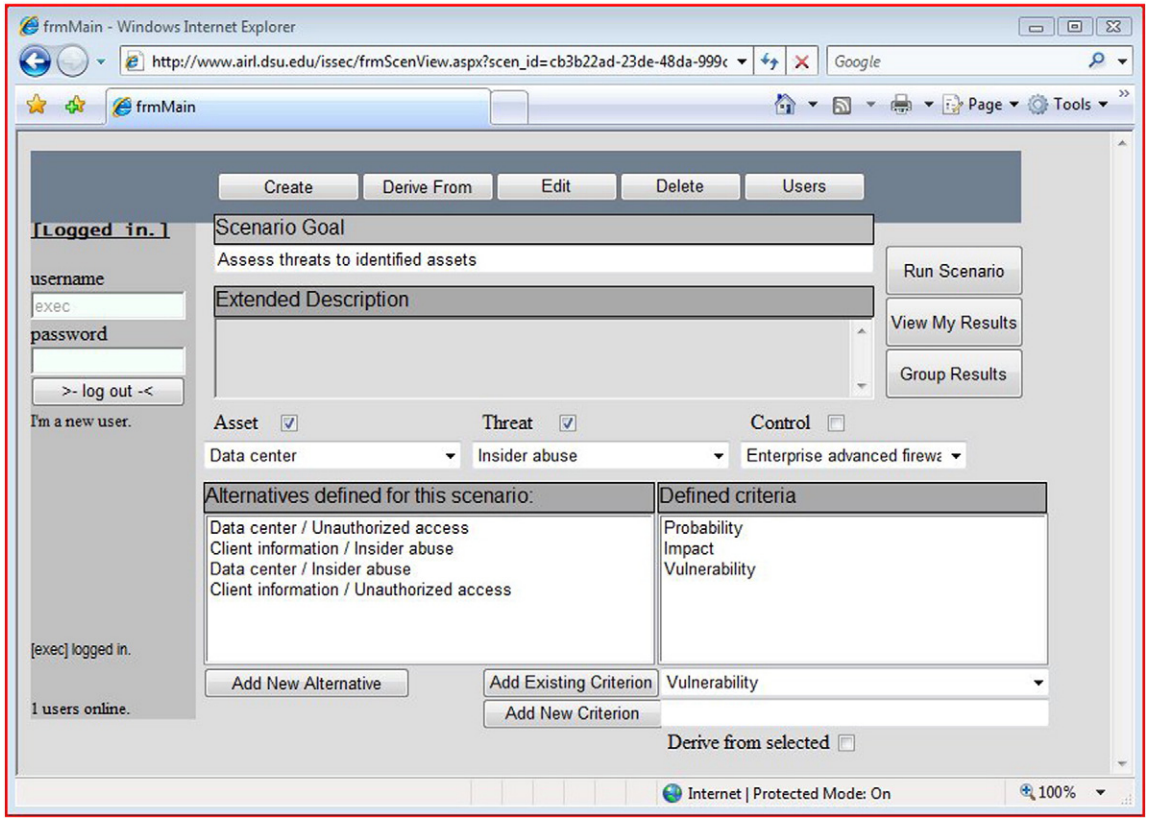


Fig. 3. Structure of the risk assessment scenario.

Table 1
Individual and aggregate results or risk assessment with contingent weightings.

	Stakeholders			Aggregates		
	Executive	Technical	Legal	Equal weighting	60% Exec 20% Tech 20% Legal	20% Exec 60% Tech 20% Legal
Criteria						
Impact	0.658	0.198	0.232	0.366	0.481	0.297
Vulnerability	0.269	0.083	0.700	0.350	0.318	0.244
Probability	0.073	0.719	.0.068	0.284	0.201	0.459
Alternatives						
Client information vs. Insider abuse	0.587	0.352	0.534	0.518	0.546	0.463
Client information vs. Unauthorized access	0.226	0.053	0.061	0.056	0.054	0.057
Data center vs. Unauthorized access	0.135	0.461	0.108	0.235	0.231	0.309
Data center vs. Insider abuse	0.052	0.134	0.297	0.191	0.169	0.171

access" (by Legal). The Technical group strongly favors the criterion of Probability (the likelihood of threat occurrence compromising the given asset). The dominant alternative is "Data center/Unauthorized access", followed by "Client information/Insider abuse". It is reasonable to believe that Technical personnel, as the people who would be asked to implement the control, would be most concerned with common threats, Executives with the possible impact on the bottom-line of their firm, and Legal with vulnerability of the assets resulting in liability to the firm.

Table 1 provides the result of aggregating stakeholders' input under three weighting structures. This reflects a situation in which the scenario owner may wish to examine alternate stakeholders' weightings to assess the robustness of the solution. With all stakeholders assigned equal weights, "Client information/Insider abuse" and "Data center/Unauthorized access" exhibited the highest risk. The ranking of the two highest risks were insensitive to changes in the stakeholders' weightings. Fig. 5 depicts the aggregate results with equal weightings. The scenario owner accepts and publishes the result, opening it to feedback by the respective stakeholders to vote on (approve or reject) the result. In the event that consensus cannot be reached, the process of preference elicitation can be returned to.

Having completed asset identification and threat assessment, the organization is now able to conduct a control selection for the most prevalent asset–threat pairs identified and prioritized through the previous stages. A single-stakeholder scenario is created which involves all stakeholder groups (Executives, Legal, and Technical) involved in the final decision in consultation with one another in a group setting, taking a single input to the system based on group consensus. The scenario organization is presented in Fig. 6. Following

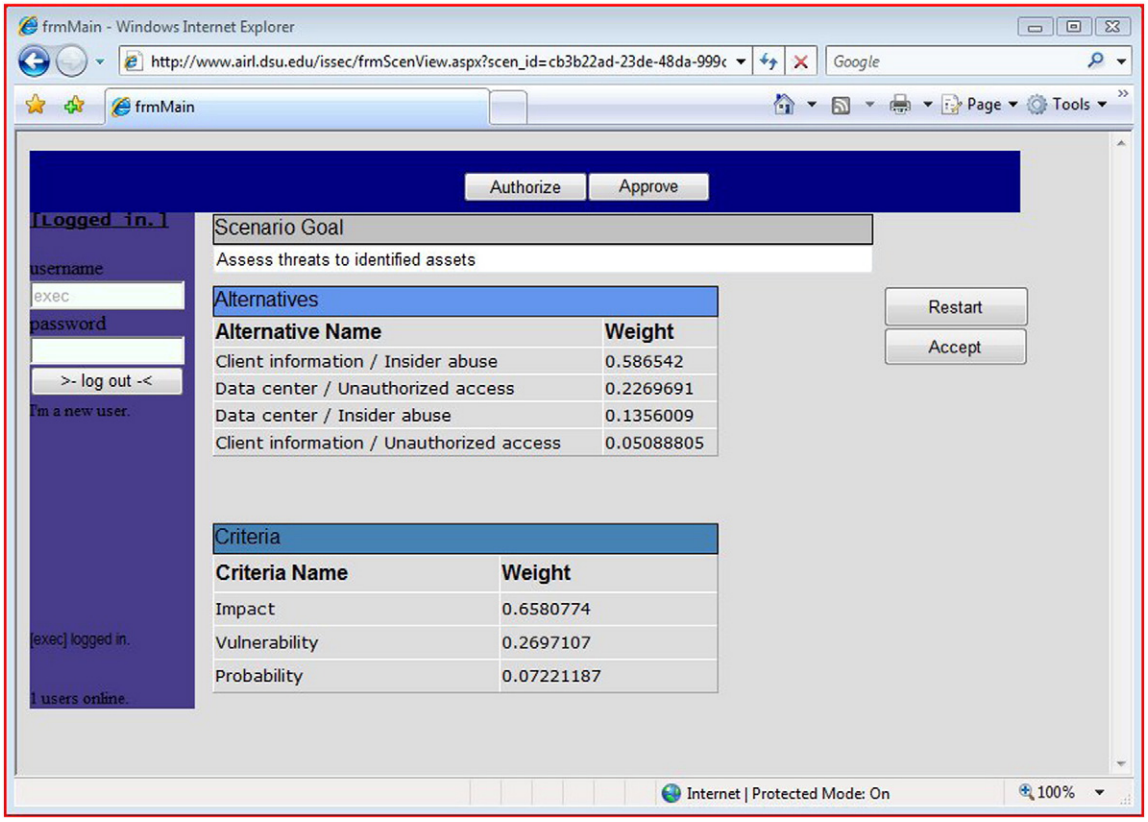


Fig. 4. Results of risk assessment for the Executive group.

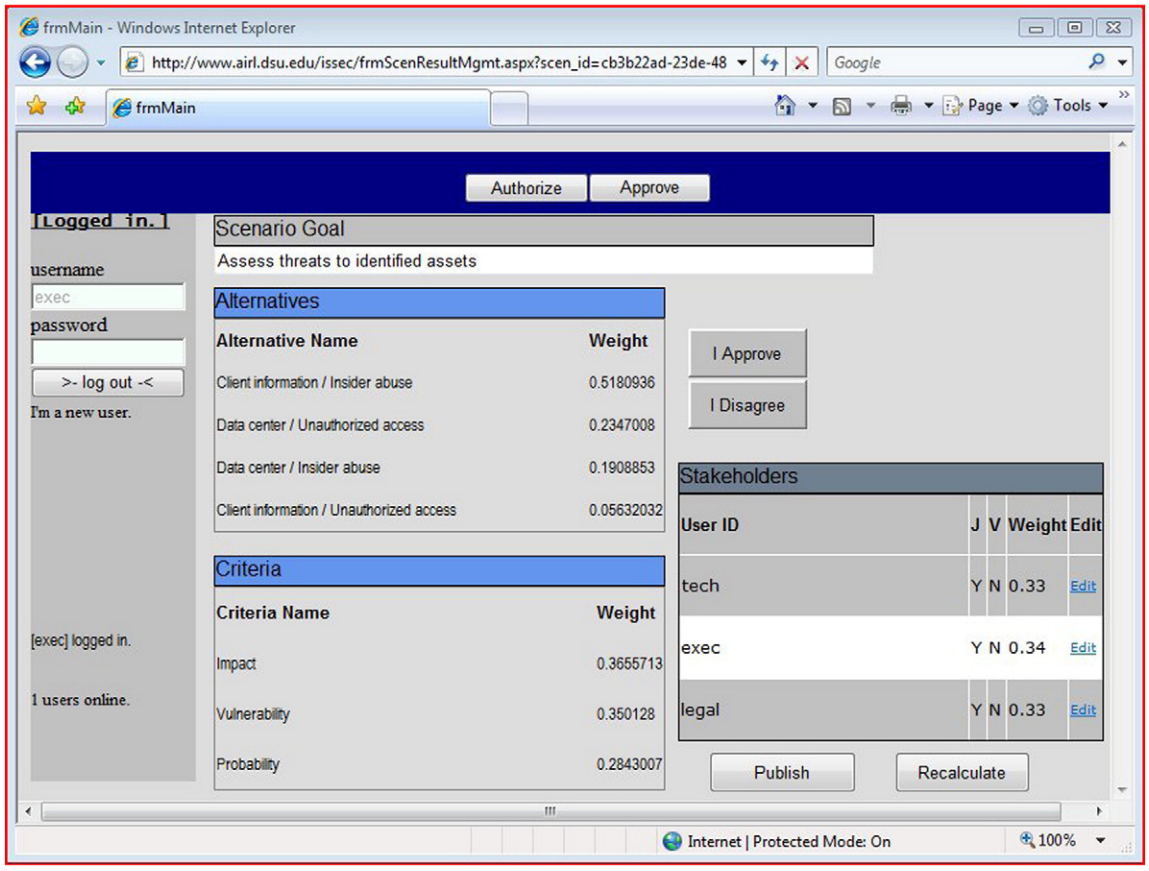


Fig. 5. Aggregated results of the risk assessment scenario.

countermeasure theory and Jones and Ashenden [27], the criteria of evaluation are:

- "Deterrence": The impact of control visibility in deterring the threat source from the asset.
- "Protection": Capacity of the control to eliminate or reduce asset vulnerability to the threat.
- "Detection": The ability of the control to recognize the occurrence of the threat to the asset.
- "Reaction": Ability of the control to mitigate risk to the asset from threat instance.

The group strongly identifies "Protection" as the most important criterion followed in order of significance, by "Deterrence", "Reaction", "Detection". Based upon the criteria structure, the group favors "Data center/Unauthorized access/Biometrics", strongly preferred over remaining alternatives. The system recommendation in effect is showing a prioritized set of recommendations on the most effective manner to defend the identified assets against most prevalent threats specific to that asset, for the control that has been determined to be most effective in addressing the stakeholder criteria preference structure. This group feels that Biometrics would be most effective in guarding the data center from unauthorized access, while the same control would be very ineffective in preventing an insider from taking advantage of his position in the organization to exploit client information, instead prioritizing "Security policy" and "Employee education" as the most efficient alternatives. The priority here applies to the entire security triplet (Asset, threat, control), ranked against one another, so the data is actionable in a variety of ways — it embeds the most efficient response to a threat–asset pair, the most significant threats, the most critical asset, all within the context of the scenario, and derived from the results of a progressive series of analysis models which become part of the aggregate judgment.

After the scenario owner closes the scenario to new judgments, the scenario can no longer be modified or take new consensus results. The given scenario becomes part of the archived knowledge base, and may be used to suggest appropriate scenario elements for future use, as well as being available to consult for future reference, along with the final judgment results for each of the individual stakeholders, allowing the user to dynamically conduct judgment sensitivity analysis on historical scenarios at a later time, and after the results have been archived.

6. Discussion and evaluation

Following a design science research methodology [22,41,61] the paper highlights the relevance of the problem and presents the theoretical principles underlying the design and development of the proposed artifact (system). To evaluate the proposed artifact, a number of design evaluation methods and patterns exist. Examples include demonstration, logical reasoning, benchmarking, using metrics, simulation, and experimentation [61]. Evaluation may involve comparison of requirements (objectives of the proposed solution) with actual observed results from use of the artifact in a demonstration [41]. The intent is to demonstrate that the system is realizable and capable of meeting the requirements as outlined in steps 4 and 5 of the design science research method [41].

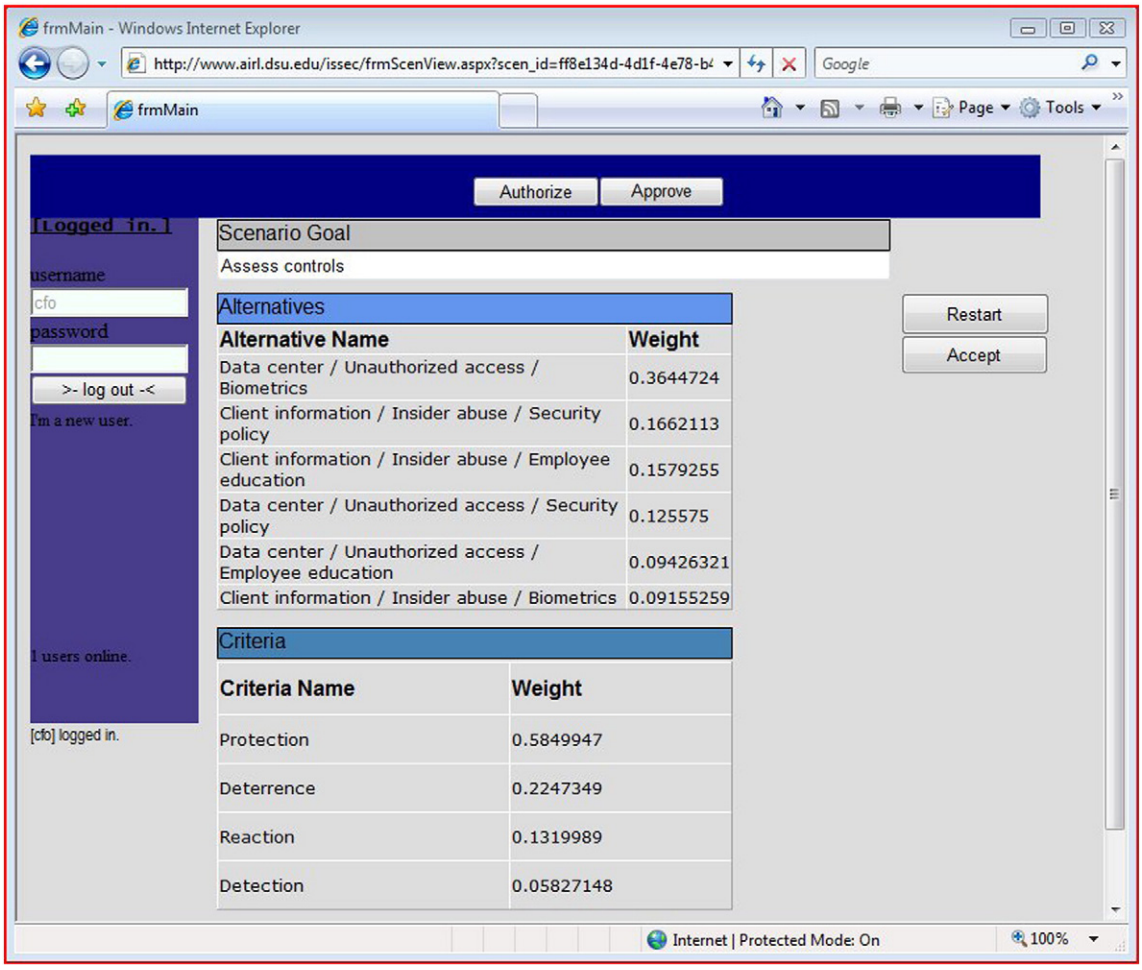


Fig. 6. Results for the control (countermeasure) selection for the collective group input.

Comparing the objectives set forth for the system in the form of system requirements with the actual behavior of the system we note the following:

A. *Support multiple stakeholder perspectives (Kantian inquiry) and subjective perceptions*: This is captured in the ability to incorporate multiple stakeholders in scenarios, and the use of AHP as an MCDM method capable of supporting subjective/qualitative preferences. Scenarios in the demonstration relate several functional groups in two distinct manners: individual preference aggregation, and group decision. The scenarios give instances of qualitative criteria such as vulnerability, and difficult-to-quantify criteria such as Impact for a threat and Deterrence for a control.

B. *Capture individual judgments which may conflict or cohere (Hegelian inquiry):* Handling conflicting judgments in trade-offs is captured in the use of AHP. Preferences for conflicting stakeholder judgments are captured by the system and available to future inquiry. In threat assessment, stakeholder preferences varied considerably — Executives were most concerned with Impact and losses, Technical group with Probability of threat, and Legal with asset Vulnerability. When assessing risk, the technical solution of biometrics was preferred for guarding the data center from unauthorized access, while policy alternatives were seen as ineffective. On the other hand, in guarding the intangible "Client information", policy and education were preferred as means to alleviate risk.

C. *Incorporate means of aggregating these preferences and evaluating the outcome*: The system uses weighted arithmetic mean method (WAMM) with support for examining alternative stakeholder hierarchies to see relationships of preference structures and assess robustness and consistency of the aggregate decision, which can be applied dynamically. In the risk assessment, independent stakeholder group preferences were aggregated, and two alternate weightings were examined to show robustness of the topmost threat–asset combination prior to the scenario owner publishing the results. In the control selection, a group working collaboratively resulted in favoring security policy and employee education as the preferred measures.

D. *Accommodate ill-structured or semi-structured problems requiring open systems and iterative judgments involving multiple and often conflicting criteria*: The design of the scenario presents a generalized goal (control selection) across several decision hierarchies and involving disparate groups of stakeholders. The overall goal is broken down in terms of an iterative set of model involving different functional groups and areas of expertise, building on the previous judgments. Independent criteria hierarchies and lists of alternatives are shown for the models which serve to narrow the scope of further inquiry to critical elements, within a broad analytical framework.

E. *Facilitate 'organizational memory' through the storage and recall of previous judgments*: Past scenarios, e.g., asset and threat assessment can be reviewed and built upon to analyze more complex scenarios Also, as mentioned in (D), the scenario demonstrates how the results of prior judgment can inform and limit the scope of higher-level scenarios.

F. *Encourage consensus formation through repeated iterations and compromises*: The system allows stakeholders to evaluate the results. Stakeholders may use the results to facilitate further discussion and decide if additional rounds of judgment are needed.

Finally, scenario results are available even for unresolved scenarios, allowing for future introspection as to why the scenario was unsuccessful, knowledge which may inform future scenario design for a similar situation.

G. *Disseminate approved outcome of the decisions made to support future judgments and scenario creation*: The online, web-based system allows authorized users to see the historical results of scenarios they have been involved in or managed, which have closed with stakeholder consensus. The scenario explicitly shows an instance of how the results of past judgments can be used in support of higher-level scenarios based on prioritized elements, and as an indirect learning process where it is the responsibility of the scenario owner to search the knowledge base for relevant information and assessment of historical scenario results.

7. Conclusion and future work

In this paper, we present a decision support system for information systems security planning. The system is capable of addressing multiple perspectives prevalent in inquiring organizations, including qualitative value judgments. This is accomplished through the development and use of a MCDM model in a web-based group decision making environment. In framing security decision making as an MCDM problem that captures the subjective perceptions of organizational stakeholders, we establish the foundation of a multi-perspective approach able to address the needs of inquiring organizations. The analysis space of asset, threat, control and combinations thereof gives a structural framework that is meaningful to security management and facilitates actionable outcomes resulting from a decision. Qualitative MCDM based on AHP models of parts of this analysis space allow us to capture subjective preferences of these stakeholders, and, layered with group support techniques for dealing with conflict and facilitating consensus as well as stakeholder preference aggregation, we are able to address the requirements of such a multi-perspective approach for the inquiring organization.

Through the scenario, we can see the trade-offs in a decision fairly explicitly through this type of approach. Even within our decision scenario, priorities become apparent, which affect the final decision outcome based on user preferences. As a technique for asset prioritization, risk assessment and control selection, this approach offers advantage over traditional techniques such as expected value or annualized loss expectancy, if the decision entails prioritization on the basis of qualitative criteria, such as capabilities or properties/attributes of the alternatives in the selection decision which are value-based or otherwise subjective in nature. The ability to represent these criteria offers advantage over checklist-based and matrix-based approaches and the system can deal with conflicting priorities. We believe it can be a valid approach in combination with quantitative techniques, used to weight the relative importance of quantitative data relative to other criteria, or simply used in parallel with quantitative risk analysis, and could be highly effective in forming a convenient summary of stakeholder opinions on an issue or problem being faced by the organization.

However, while the proposed system provides a foundation for security planning in inquiring organizations, issues pertaining to managing the potential complexity of the resulting decision space are warranted. This may be accomplished by using the rating method in AHP as well as exploring alternative MCDM methods. Further work is also needed to explore ways for integrating the proposed system with existing security planning methodologies and approaches in a complimentary manner. With respect to group support, there are opportunities to utilize more sophisticated methods of aggregation. Exploration of the application of some of these techniques is expected.

Further work is also needed for field testing and evaluation of the proposed system. In this research we have demonstrated and evaluated the use of the proposed system in addressing problems encountered in security planning. In that regard, we have compared the systems' functionality with the solution objectives as noted in Peffers et al. [41]. The next step is a comprehensive evaluation of the system in the field. This can take the form of a single or multiple case studies that documents the usage of the system in one or more organization. Alternatively, such field testing may involve a quantitative evaluation of the usability and acceptance of the system. An example of such study is conducted by Hu et al. [24] where they evaluate the acceptance of COPLINK, a web-based knowledge management system for law enforcement.

There are also issues with anonymity of user input. There are pros as well as cons of making participants anonymous at group meetings [13]. In that regard, the system guarantees the anonymity among participants. Individual participants have access to their preferences as well as to the group (aggregated results). They do not have access to other participants' input or preference structure. However, to aggregate individual preferences in order to obtain the group's composite priorities, we need to provide individual participants' weights (if they are not to be equally weighted). Such an approach will necessitate that the creator (owner) of the scenario be able to set the individual weights. By manipulating the weights, the creator of the scenario may indirectly infer the final evaluation of individual participants (criteria and alternative rankings). However, the creator does not have access to the judgments made by individual participants. We have opted to allow the creator/owner of the scenario to manipulate individual weights (as opposed to assuming equal weights) to address some of the concerns raised in [13], such as to allow the scenario creator to capture experience, expertise, and knowledge into the decision process. An underlying assumption is that the scenario creator is in the best position to make such judgment. Regardless, further research is warranted in the efficacy of partially compromising creator–participant anonymity for the flexibility in manipulating individual participants' weights.

In conclusion, as information systems security encompasses an ever-greater scope of organizational relevance and responsibility, it becomes necessary for us to develop decision support methodologies and ultimately, systems, capable of dealing practically with the complex and multifaceted nature of the decision making of information systems security entailed by emerging notions of a "new paradigm" for security within the inquiring organization — systems which, in turn, can aid in facilitating higher levels of organizational inquiry necessary to deal with this level of complexity. It is not unreasonable to suggest that the significance of information systems security will continue to dominate the organizational landscape. The challenges to meet the expectations of organizations and society as a whole will continue to be a major concern for security planners and decision makers. Information system security planning methodologies and decision support tools will need to continue to evolve if we are to be capable of meeting such demands as those elucidated in this paper, and we would suggest that the system prototype presented is an early step in that direction.

Acknowledgments

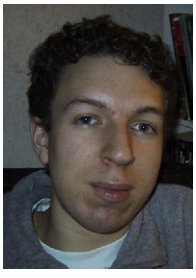
The authors would like to thank a financial service provider for their input and continued interest in this project, as well as colleagues who have provided us with additional feedback and suggestions as this work has progressed.

References

[1] J. Aczel, T. Saaty, Procedures for synthesizing ratio judgments, Journal of Mathematical Psychology 27 (1) (1983) 93–102.
[2] A. Arbel, R. Tong, On the generation of alternatives in decision analysis problems, Journal of the Operational Research Society 33 (1982) 377–387.
[3] R. Baskerville, M.T. Siponen, An information security meta-policy for emergent organizations, Journal of Logistic Information Management (2001).
[4] L.D. Bodin, L.A. Gordon, M.B. Loeb, Evaluating information security investments using the analytic hierarchy process, Communications of the ACM 48 (2) (2005).
[5] R. Bojanc, B. Jenman-Blazic, Towards a standard approach for quantifying an ICT security investment, Computer Standards & Interfaces 30 (4) (2008) 216–222.

[6] N. Bryson, Group decision-making and the analytic hierarchy process: exploring the consensus-relevant information content, Computers & Operations Research 23 (1) (1996) 27.
[7] H. Cavusoglu, B. Mishra, S. Raghunathan, A model for evaluating IT security investments, Communications of the ACM 47 (7) (2004) 87.
[8] C.W. Churchman, The Design of Inquiring Systems: Basic Concepts of Systems and Organizations, Basic Books, New York, NY, 1971.
[9] J.F. Courtney, Decision making and knowledge management in inquiring organizations: toward a new decision-making paradigm for DSS, Decision Support Systems 31 (1) (2001) 17–38.
[10] R.F. Dyer, E.H. Forman, Group decision support with the analytic hierarchy process, Decision Support Systems 8 (2) (1992) 99–123.
[11] T. Efraim, J. Aronson, T.P. Liang, R. Sharda, Decision Support and Business Intelligence Systems, 8 ed.Prentice Hall, Upper Saddle River, NJ, 2007.
[12] J. Eloff, M. Eloff, Information security management — a new paradigm, presented at Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology, 2003.
[13] M.C. Er, A.C. Ng, The anonymity and proximity factors in group decision support systems, Decision support system 14 (1995) 75–83.
[14] M.T. Escobar, J.M. Moreno-Jimenez, Aggregation of individual preference structures in AHP-group decision making, Group Decision and Negotiation 16 (2007) 287–301.
[15] T. Finne, The three categories of decision-making and information security, Computers & Security 17 (5) (1998) 397–405.
[16] E.H. Forman, Facts and fictions about the analytic hierarchy process, Mathematical Computer Modeling 17 (4–5) (1993) 19–26.
[17] S. Frosdick, The techniques for risk analysis are insufficient in themselves, Disaster prevention and management 6 (3) (1997) 165–177.
[18] G. Gaskell, "Simplifying the Onerous Task of Writing Security Policies," presented at First Australian Information Security Workshop, Deakin University, Geelang, Victoria, 2000.
[19] M. Gerber, R. von Solms, Management of risk in the information age, Computers & Security 24 (1) (2005) 16–30.
[20] L.A. Gordon, M.B. Loeb, The economics of information security investment, ACM Transaction on Information System and Security 5 (4) (2002) 438–457.
[21] S.J. Greenwald, Discussion Topic: What is the old security Paradigm? presented at Proceedings of the New Security Paradigms Workshop, Charlottesville, Virginia, 1998.
[22] A.R. Hevner, S.T. March, J. Park, S. Ram, Design science in information systems research, MIS Quarterly 28 (1) (2004) 75.
[23] L.J. Hoffman, Risk analysis and computer security: towards a theory at last, Computers & Security 8 (1) (1989) 23–24.
[24] P.J.H. Hu, User acceptance of intelligence and security informatics technology: a study of COPLINK, Journal of the American Society for Information Science and Technology 56 (3) (2005) 235–244.
[25] C.L. Hwang, K. Yoon, Multiple attribute decision making: methods and applications, Springer-Verlag, Berlin, Germany, 1981.
[26] P. Jager, The myth of technical security, *American Bankers Association*, ABA Banking Journal 96 (1) (2004) 8.
[27] A. Jones, D. Ashenden, Risk Management for Computer Security, Elsevier Butterworth-Heinemann, Burlington, MA, 2005.
[28] P.M. Kort, J.L. Haunschmied, G. Feichtinger, Optimal firm investment in security, Annals of Operations Research 88 (1999) 81.
[29] J. Leach, Security engineering and security ROI, Computers & Security 22 (6) (2003).
[30] H.A. Linstone, Multiple Perspectives for Decision Making, North-Holland, New York, 1984.
[31] J.G. March, Z. Shapira, Managerial perspectives on risk and risk taking, Management Science 33 (11) (1987) 1404.
[32] R.O. Mason, I.I. Mitroff, Challenging Strategic Planning Assumptions, Wiley, New York, 1981.
[33] Mercuri, Analysing security costs, Communications of the ACM 46 (6) (2003).
[34] I.I. Mitroff, H.A. Linstone, The Unbounded Mind: Breaking the Chains of Traditional Business Thinking, Oxford University Press, New York - Oxford, 1993.
[35] C. Muralidharan, N. Anantharaman, S.G. Deshmukh, A multi-criteria group decision making model for supplier rating, Journal of Supply Chain Management 38 (4) (2002) 22–33.
[36] J.F. Nunamaker, R.O. Briggs, D.R. Mittelman, Lessons from a decade of group support systems research, presented at Hawaii International Conference on Systems Science (HICSS), Hawaii, 1996.
[37] D.L. Olson, Decision Aids for Selection Problems, Springer-Verlag, New York, 1996.
[38] D.L. Olson, A.I. Mechitov, H. Moshkovich, Comparison of AHP with six other selection aids, presented at Fouth International Conference on AHP, Burnaby, BC, 1996.
[39] D.L. Olson, M. Venkataramanan, J.L. Mote, A technique using analytical hierarchy process in multi-objective planning models, Socio-economic Planning Sciences 20 (6) (1986) 361–368.
[40] D. Parker, The strategic values of information security in business, Computers & Security 16 (7) (1997) 572–582.
[41] K. Peffers, T. Tuunanen, M. Tothenberger, S. Chaterjee, A design science research methodology for information systems research, Journal of Management Information Systems 24 (3) (2008) 45–77.
[42] D. Petkov, O. Petkova, T. Andrew, T. Nepal, Mixing multiple criteria decision making with soft systems thinking techniques for decision support in complex situations, Decision Support Systems 43 (4) (2007) 1615–1629.
[43] S.L. Pfleeger, R. Rue, Cybersecurity economic issues: clearing the path to good practice, IEEE Software 25 (1) (2008) 35–42.
[44] S.A. Purser, Improving the ROI of the security management process, Computers & Security 23 (7) (2004) 542–546.
[45] R. Ramanathan, L.S. Ganesh, Group preference aggregation methods employed in AHOP: an evaluation and intrinsic process for deriving members' weightages, European Journal of Operational Research 79 (1994) 249–265.
[46] R. Richardson, 2008 CSI Computer Crime and Security Survey, Computer Security Institute, 2008.
[47] S.M. Richardson, J.F. Courtney, D.B. Paradice, An assessment of the Singerian inquiring organizational model: cases from academia and the utility industry, Information Systems Frontiers 3 (1) (2001) 49.
[48] H.W. Rittle, M.M. Webber, Dilemmas in a general theory of planning, Policy Sciences 4 (1973) 155–169.
[49] J. Ryan, D.J. Ryan, Expected benefits of information security investments, Computers & Security 25 (8) (2006) 579–588.
[50] T. Saaty, The Analytic Hierarchy Process, McGraw-Hill, New York, 1980.
[51] P. Senge, J. Sterman, Systems thinking and organizational learning: acting locally and thinking globally in the organization of the future, European Journal of Operational Research 59 (1) (1992) 137–150.
[52] H. Simon, The New Science of Management Decision, Harper and Brothers, New York, NY, 1960.
[53] M.T. Siponen, Five dimensions of information security awareness, ACM SIGCAS Computers and Society 31 (2) (2001) 24–29.
[54] B. Srdjevic, Linking analytic hierarchy process and social choice methods to support group decision-making in water management, Decision Support Systems 42 (2007) 2261–2273.
[55] E. Stein, V. Zwass, Actualizing organizational memory with information systems, Information Systems Research 6 (2) (1995) 85–117.
[56] T. Stewart, A critical survey of the status of multiple criteria decision making theory and practice, OMEGA 20 (5–6) (1992) 569–586.
[57] D.W. Straub, R.J. Welke, Coping with systems risk: security planning models for management decision making, MIS Quarterly 22 (4) (1998) 441–469.
[58] Strutt, Risk assessment and management: the engineering approach, Center for Industrial Safety and Reliability, Cranfield University, 1993.
[59] L.L. Sun, R.P. Srivastava, T.J. Mock, An information systems security risk assessment model under the Dempster–Shafer theory of belief functions, Journal of Management Information Systems 22 (4) (2006) 109–142.
[60] M. Tavana, Cross: a multicriteria group-decision-making model for evaluating and prioritizing advanced-technology projects at NASA, Interfaces 33 (3) (2003) 40.
[61] V. Vaishnavi, W.J. Kuechler, Design Science Research Methods and Patterns: Innovating Information and Communication Technology, Auerbach Publications - Taylor & Francis Group, Boca Raton, FL, 2008.
[62] L.G. Vargas, An overview of the analytic hierarchy process and its applications, European Journal of Operational Research 48 (1990) 2–8.
[63] P. Vihakapirom and K. Li, A Framework for Distributed Group Multi-Criteria Decision Support Systems., Retrieved from http://ausweb.scu.edu.au/aw03/papers/li/paper.html on (February 2004).
[64] R. Willison, J. Backhouse, Understanding criminal opportunity in the is context, presented at IRIS, Finland, 2003.
[65] W.T. Yue, M. Cakanyildirim, Y.U. Ryu, D. Liu, Network externalities, Layered Protection and IT Security Risk Management, Decision Support Systems 44 (1) (2007) 1–16.
[66] A. Zuccato, Holistic security requirement engineering for electronic commerce, Computers & Security 23 (1) (2004) 63.

Dr. El-Gayar is a Professor of Information Systems at the College of Business and Information Systems and the Dean of Graduate Studies and Research at Dakota State University. His research interests include: decision support systems, multiple criteria decision making, and the application of decision technologies in security planning and management, healthcare, and environmental management. He has an inter-disciplinary educational background and training in information technology, computer science, economics, and operations research. In addition to his academic credentials, Dr. El-Gayar has industry experience as an analyst, modeler, and programmer. He has numerous publications in the various information technology related fields. He is a member of AIS, ACM, INFORMS, and DSI.



Brian D. Fritz holds an M.S. in Information Systems from Dakota State University, with undergraduate from South Dakota State University and is a past or present member of ACM, AIS, Decision Sciences Institute (DSI), The Data Warehousing Institute, and ICCP. He is currently employed in the private industry as a CRM and data specialist in the electrical manufacturing sector, and an occasional consultant. Research interests include CRM, decision support, data mining, and inquiring systems, as well as philosophy of information systems.