2005

ISSEC: A socio-technical DSS for information security planning

Brian D. Fritz
Dakota State University

Omar F. El-Gayar
Dakota State University

1-1-2005

ISSEC: A Socio-technical Decision Support System for Information Security Planning

Brian D. Fritz
Dakota State University, fritzb@pluto.dsu.edu

Omar El-Gayar
Dakota State University, omar.el-gayar@dsu.edu

ISSEC: A socio-technical decision support system for information security planning

Brian D. Fritz
College of Business and Information Systems
Dakota State University
fritzb@pluto.dsu.edu

Omar F. El-Gayar
College of Business and Information Systems
Dakota State University
omar.el-gayar@dsu.edu

ABSTRACT

The traditional notion of information security, rooted in a solidly technical foundation, has within the past decade seen wide criticism within academia - much of which has originated from the social sciences community - as being narrow and technology-centric instead of holistic and organizational in its focus. As information security awareness encompasses an ever-greater scope of organizational dynamics, it becomes necessary for us to develop design methodologies and ultimately, systems, capable of dealing practically with the complex and multifaceted nature of the decision-making of information systems security which is entailed by the emerging notions of a new paradigm for security.

To this end, we present an architecture which implements a web-based multi-user decision support system (DSS) driven by an operational security model within a qualitative multi-criteria framework that utilizes AHP as its inference engine. The system is then demonstrated in action, by addressing a multi-criteria security control selection decision.

Keywords

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

INTRODUCTION

Recent figures suggest that losses from security breaches continue to be a major organizational concern. Well-known polls such as that conducted by the Computer Security Institute (CSI) in collaboration with the Federal Bureau of Investigation (FBI), published in 2002 (Power, 2002) and 2003 reported significant losses to the polled organizations due to security incidents, with 56% of organizations surveyed reporting detected security breaches. Moreover, PricewaterhouseCoopers L.L.P. and Information Week, reported an estimated $1.6 trillion dollars in damage on the global economy and $266 billion within only the United States (Cavusoglu, Mishra, Raghunathan, 2004). Such numbers should serve to convey to us a clear signal that security remains a continually significant issue with organizational as well as economic impacts. This is further evidenced in the increasing focus which information security is receiving in the legal environment (Smedinghoff, 2005).

However, security literature and theory has in the past decade come under wide criticism, as being largely technocratic (e.g., Willison and Backhouse, 2003) and functionalistic in its approach to information security, at the expense of the organizational aspect (Jager 2004). The multidimensional nature of security awareness (Siponen 2001) precludes, from this perspective, the ability of traditional security management approaches to consider significant factors that are not easily quantifiable, within their decision-making. The traditional focus, represented best by the so-called "C.I.A." paradigm of Confidentiality, Integrity, Availability (Greenwald 1998), has historically been on the "Confidentiality" aspect of the triad – the preservation of secrecy, development of increasingly sophisticated security technologies and encryption capabilities. Proponents of organizational, behavioristic, and socio-technical orientations purport that such a focus places undue emphasis on the role of technology at the expense of a wider organizational context full of actors who can and do influence the technology which becomes embedded in the organization.

Within this paper, we seek to address the viability of a re-orientation of security management decision-making along more behavioral and organizational lines, specifically through the development of a collaborative decision support system (DSS) for security decision-making and planning, which incorporates notions drawn from group decision making, multi-criteria decision analysis and inquiring systems through the implementation of an multiple criteria decision making (MCDM) framework incorporated by the authors into a distributed web application.

The paper is organized as follows: the next section provides a brief review of relevant literature. We then present a

description of the proposed architecture, briefly discuss our implementation, and follow with a case study demonstrating the applicability of the proposed system in addressing concerns identified in the literature. The final section concludes the paper with reflections and direction for future research.

LITERATURE REVIEW

This work draws its theoretical foundation from several disparate research areas, underscoring the multidisciplinary nature of such attempts to synthesize technical and organizational concerns into a coherent whole. The adoption of a socio-technical perspective towards decision-support systems (Sena and Shani, 1999) and deliberate inclusion of socio-technical design principles (Mumford, 1996) into the architecture of such a DSS is to the best of our knowledge an unexplored domain of research. The following sections presents a brief review of security planning and decision making, and theoretical contributions in inquiring systems and organizational learning, upon which this research is grounded.

Security planning and decision making

The literature identifies a severe disconnection between strategic and operational decisions (Rees, Bandhopadhay, Spafford 2003; Baskerville and Siponen, 2001) and, in consequence, an ad-hoc and reactive approach to security policy-making (Gaskell, 2000) focused around the needs and concerns of the present moment with little regard for maintaining consistency in security policy. Of course, this generalization cannot be applied unilaterally; nonetheless, the distinction receives support from empirical security assessment surveys (i.e. Whitman, 2003; Power, 2002). This is in part due to the rapid pace of technological innovation and consequent lag in organizational policy adaptation (Baskerville and Siponen, 2001), but we would suggest it is symptomatic of a systematic lack of proper and efficient communication between executive and operational personnel with respect to the security environment.

Security management has come to be regarded as largely a subset of risk management, and quantitative and mathematical analysis approaches to security investment and management have been heavily emphasized (i.e., Kort, Haunshmied, and Feichtinger, 1999; Courtney, 1977). Modern techniques available to risk management are designed to work with high-level aggregate data, which makes them often troublesome to many IT security considerations (Cavusoglu, Mishra, and Raghunathan, 2004) which occur within the organization at the operational level.

The literature offers us some avenues of approach to the formalization of security decision-making (Baskerville, 1993) and security management (Straub and Welke, 1998) which reach beyond the level of risk management through checklist-like approaches and access control matrices (Lampson, 1977; Bell and LaPadula, 1976), techniques developed in the infancy of information security and which are still in use today in modern standards like ISO 17799. Building upon these initial approaches which first introduced basic decision theory concepts into information security management, (El-Gayar and Fritz, 2004) extended the application of decision theory to multi-criteria decision-making (MCDM) and advanced a preliminary framework for decision support incorporating these ideas into an analysis space suitable for multidimensional security analysis, but lacked a solid theoretical grounding for proposing a system which supported these notions.

Inquiring systems and organizational learning

Churchman's seminal work on inquiring systems (Churchman, 1971) provides us with a comprehensive framework for defining intelligence in systems, and thus, for valid approaches to complex problems. Alternatives to a normative Leibnitzian rational philosophy, which he defines as Lockean (empirical objectivity), Kantian (multi-perspective), Hegelian (dialectical or conflict-based), and Singerian (learning through gradual discernment of cause and effect based on success of past outcomes) are identified as useful approaches to issues which are peculiarly complex, in that their analysis requires the consideration of ill-defined problems, heterogeneity of levels of communication, and highly context-dependent concerns where objectivity is difficult or impossible, and reliance upon subjective judgment (at and above the "Kantian" mode of inquiry) and thus on *a posteriori* as well as *a priori* reasoning.

We can take it for granted that each decision-maker avails himself of some amount of intelligence in regard to the surrounding environment, which he then uses in making a decision. Our ability to progress beyond this statement to a universal assumption is, however, limited a priori outside the Leibnitzian paradigm implicitly assumed by rational choice theory (Olson, 2001). A socio-technical view of security necessitates a boundedly rational approach (Simon, 1960) to decision-making, given our assumption of the complex and ill-structured nature of the problem domain and our lack of complete information. This implies an inherent subjectivity of judgments expressed and thus a need for communication and collaboration between conflicting perspectives, with the intent to eventually reach an agreeable consensus.

To extend the organizational system to the Singerian mode of inquiry requires additionally the establishment of organizational memory (Stein and Zwass, 1995) by supporting the collection and aggregation of individual knowledge that is collaboratively accepted, (Richardson, Courtney, and Paradice, 2001) and facilitating its timely recall by some associative process. The facilitation of organizational learning (Senge and Sterman, 1992) 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 future decision-making.

MCDM and group decision support

Multiple criteria decision making (MCDM) would seem a natural technique to support the sort of organizational learning through group collaboration (see Nunamaker, Briggs, and Mittelman 1996) identified above. The availability, intuitive nature, and ease of use of the Analytic Hierarchy Process (AHP) technique for MCDM make it an ideal candidate for this purpose (Bryson, 1996). Briefly, AHP is an analytic technique that utilizes pair-wise comparisons between possible alternatives over a set of diverse criteria (Saaty, 1980). AHP supports qualitative comparisons (Vargas, 1990) as well as meaningful comparison given incommensurable unit measures (Hwang and Yoon, 1981). The explicit use of pair-wise comparisons means that trade-offs in conflicting judgments are made obvious to the decision-maker. The simplicity of user interaction and ability to hide the implementation details of the algorithm without adversely affecting the usability of the results increase its desirability for system implementation in this context (Vihakapirom and Li, 2003).

Group decision support through AHP is not without its difficulties, however. Adaptations of AHP to the support of a group decision making context have been made (Tavana, 2003; Muralidharan, Anantharaman, and Deshmukh, 2002), though a majority of applications focus on group collaboration as the basis of input prior to the AHP process itself, or AHP as an initial step, followed by other techniques. However, our interest lies in the combination of separate, individual and subjective judgments expressed as preference structures over a common set of criteria, which would be necessary to support the higher levels of inquiry (Kantian, Hegelian, Singerian) represented above, through group interaction which occurs after the individual (subjective and qualitative) preferences have been elicited and collected.

THE SYSTEM ARCHITECTURE

We can now deduce a number of requirements that would define the context of a socio-technical approach to decision support for information security, and thus justify the design of our proposed system. We recognize as explicit the need to accommodate multiple stakeholder perspectives, and to facilitate 'organizational memory' through the storage and associative recall of previous judgments. The system, to support Hegelian and Singerian levels of organizational inquiry (Richardson et al., 2001), would need to incorporate means of aggregating these preferences and evaluating the outcome. Finally, the approved outcome of the decisions made should be available to support future judgments and scenario creation.

A web-based distributed architecture seems a natural choice for such a situation. Associative recall suggests database technology and especially a data warehouse for archiving results permanently. The need for preference aggregation suggests that group dynamics will be important, and this in turn should be leveraged through social feedback-based processes whenever possible, to accommodate disagreement and allow the expression of stakeholder opinion in the decision. The system will support judgments that are iterative in nature.

Figure 1 provides a high-level conceptual diagram of the system under discussion. Our implementation focuses around three major functional areas: Preference aggregation, Inference engine, and Knowledge association, supported by an underlying data warehouse. This connected set of subsystems provides the infrastructure upon which the presentation-level access (i.e., the user interface) is built.

Knowledge association

Our initial model for the MCDM decision framework advocated a combinatorial approach to alternative generation, delineating a series of analysis spaces corresponding to the basic operational security notions of Asset, Threat, and Control. This system implements that model implicitly and this is reflected in the data warehouse design schema, which in turn feeds the inference engine. The Knowledge association module handles the translation of these elements into the schema of the data warehouse, generating relational links between scenarios and reusing combinations held in common between scenarios.

One of the first developments which became obvious to us in the course of system design was that the multi-criteria-based approach undertaken in (El-Gayar and Fritz, 2004) lent itself to a scenario rather than model-based approach to decision analysis. Originally we had set out to develop a model-based decision support system, but experimentation led us to realize

that a scenario-based approach allows for more detailed analysis results to be viewed on a case-by-case basis and overall, it seemed more appropriate to the nature of the inquiring system which we were attempting to produce.

The Knowledge association module maps chosen elements and criteria to existing scenarios if possible, or creating unique elements when necessary. This serves to limit greatly duplication (one of the earliest problems faced in experimenting with the initial framework using the AHP software package Expert Choice™) 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.

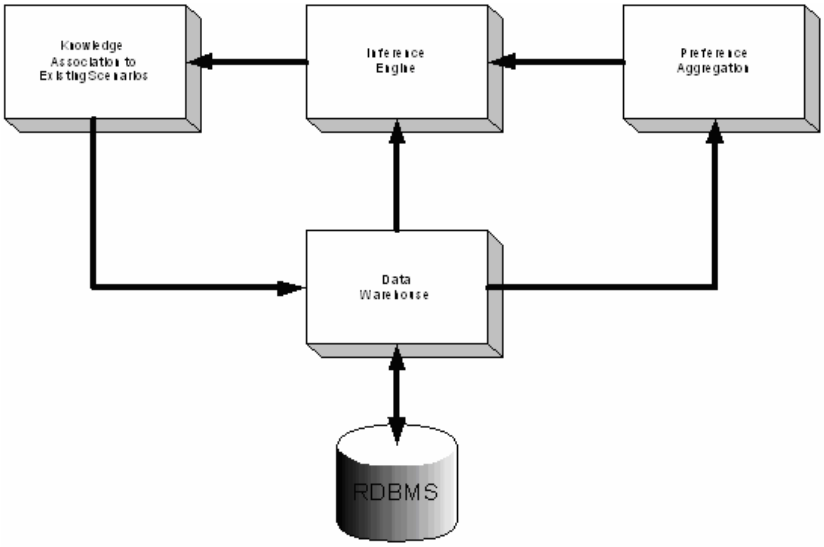

Figure 1. Architecture of the developed system.

Inference engine

The initial prototype of the system uses AHP as its inference engine, though the proposed system can be adapted to utilize different MCDM methodologies as well. Alternatives and criteria are derived through the Knowledge association module and separate judgments are stored for each stakeholder both for criteria prioritization and alternative evaluation. Due to the need for the knowledge association module and tight integration with the data warehouse, we decided to implement AHP ourselves. We chose a normalized eigenvector approach (one of the first techniques developed by Saaty (1980) and still a commonly preferred choice) due to its robustness, speed, and ease of implementation.

The AHP technique uses redundant pair-wise matrices, thus a given set of n inputs will require:

$(n^2 - n) / 2$ comparisons to be made by each stakeholder.

Thus, given an AHP scenario composed of n criteria ($C_1 \ldots C_n$) and m alternatives ($A_1 \ldots A_m$), for each stakeholder: There are

$[(n^2 - n) / 2] + [n(m^2 - m) / 2]$ judgments required.

The exponential growth resulting quickly becomes intractable from a practical standpoint, which makes the technique applied in this setting suitable for a relatively small number of inputs, again supporting our employment of a scenario-based approach to the decision analysis. This is a widely acknowledged weakness of the technique but one which can be mitigated by informed scenario design. We dynamically calculate judgments from the stored priorities, to allow for ease of adjustments when performing aggregations, as well as allowing for future integration with other data sources.

Preference aggregation

Preference aggregation in this system is two-fold. Individual preference hierarchies are combined through the assignment of stakeholder weights *w* 'democratically' (i.e. based on *m* stakeholders, each stakeholder has a share of ($w = 100\% / m$) in the decision outcome, but support for dynamic adjustment is achieved by applying the preference weight *w* to the priority associated with the preference before the preference enters the inference engine. We chose to implement the system in this way to allow for flexibility in the aggregation method used. Again, a multitude of mathematical approaches have been

postulated for group decision support, many of which aim at finding an *a priori* aggregate function for this summation in terms of utility maximization.

Our focus, however, on a socio-technical approach suggested instead that stakeholder feedback should be the prime element in the generation of consensus. To this end, we allow the scenario designer to 'publish' the aggregate result and the stakeholders are then able to vote in support of the result or to dispute it. Figure 2 depicts in an abstracted form the process of aggregation used in this system. This same technique may be applied for much more sophisticated aggregation methods without changing the underlying group dynamics in any way. Simple weighted sums allow for rapid feedback and which are applied systematically through the inference engine.

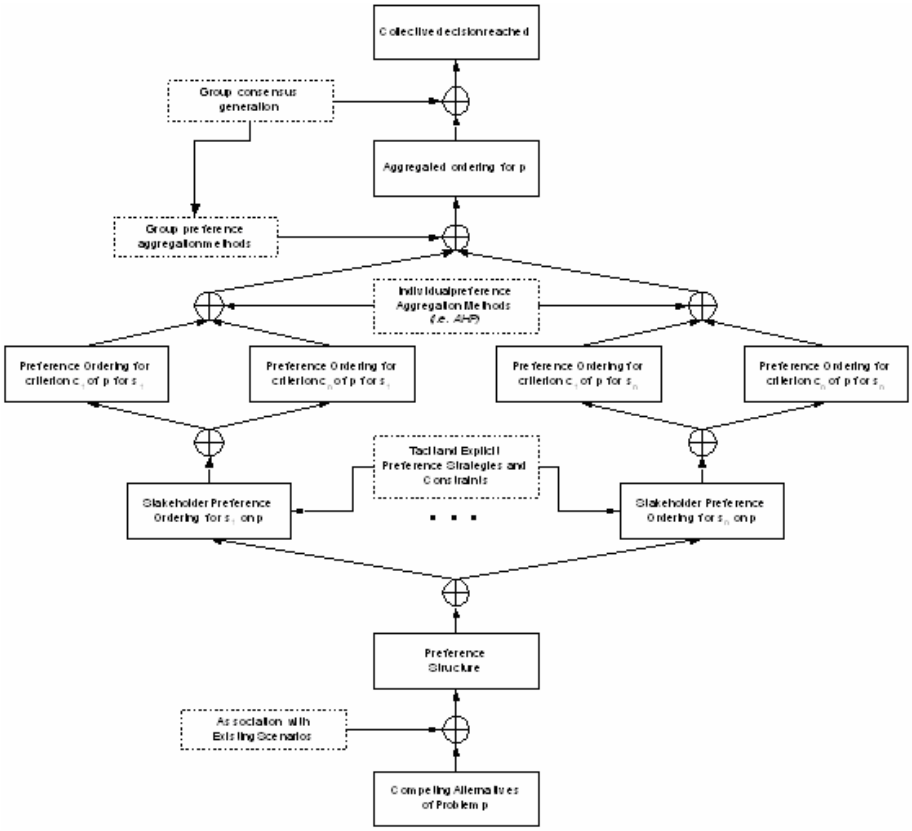

Figure 2. Stakeholder preference aggregation

Implementation details

In brief, the system uses an industry standard n-tier architecture composed of three main layers: Presentation layer (containing server-side scripting), Business layer (containing analysis objects), and Data Access layer (abstracting from a relational database management system (RDBMS) architecture and providing object-specific as well as general utility methods and connection management). Web scripting occurs in Microsoft's ASP.NET and business objects are compiled into .NET assemblies, supported by a dozen SQL stored procedures and a handful of views and functions, residing, with the data warehouse star schema, in Microsoft's SQL Server 2000.

USING THE SYSTEM

Figure 3 depicts the normal process flow for use of the implemented DSS. This diagram also describes the major components of the user interface, residing at the presentation layer of the web-based system.

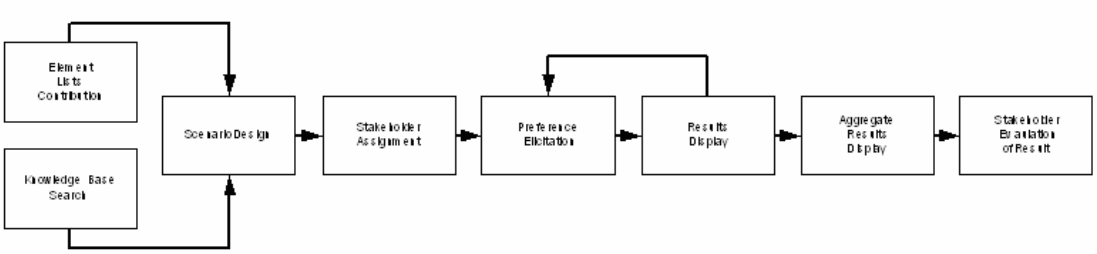

Figure 3. System flow diagram

The general procedure for using the system is as follows:

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 view 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. This information is permanently recorded.

CASE STUDY

One of the major criticisms of traditional risk-management based decision analysis is that it offers little insight into how the different factors of a security infrastructure might interact with regard to the type and quality of response which is offered given the presence of a threat. In other words, it leaves us unable to see, for example, what kinds of trade-offs are implied between various controls. A security investment decision may greatly depend upon the preference among these criteria in lieu of, or in addition to, financial considerations. The ability to discern such a preference, taking into account something of the specific nature of the controls that are being considered, could be very valuable if integrated into the selection process, as the present system attempts to do.

The scenario shows how a qualitative multi-criteria approach can address this basic problem, in addition to demonstrating the system in action. In this scenario, a small-medium enterprise (SME) is facing resource allocation decisions and wishes to put a security control into place but is unsure of its best option. They know roughly that they would prefer a preventative solution and that they are willing to spend a reasonable amount of money if required. Three stakeholders will be involved in the decision. In this case study, we follow through the general process outlined above with the creation, design, preference collection, aggregation and voting, and recall of a sample scenario. A user logs into the system and references the knowledge base (step not shown, but see Figure 8). The user determines that appropriate elements are available for the scenario, but finds no scenarios that are an appropriate basis to derive the current scenario from. The user then enters the scenario editor (Figure 4).

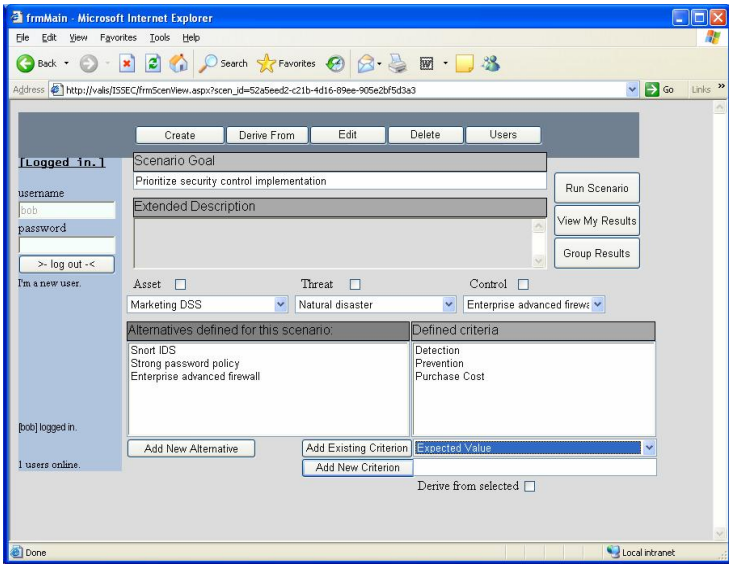

Figure 4. ISSEC-DSS: Scenario editor

The scenario creator selects the type of scenario (alternatives are single elements) and chooses appropriate alternatives from the provided list. In this case, our user chooses three controls: "Snort" (a well-known open source intrusion detection system), "Strong password policy", and "Enterprise advanced firewall". The user decides that the scenario's decision hierarchy will consist of three criteria: "Detection", "Prevention", and "Purchase Cost".

Having established the scenario and saved the structure, the user now assigns three users as decision stakeholders and then opens the scenario to receive judgments. These users now have permission to enter the scenario and input their preferences. A user logs on to the system (Figure 5) and sees the newly assigned scenario in the active scenario listing, along with another open scenario for threat evaluation, and one "Pending" work-in-progress by the user.

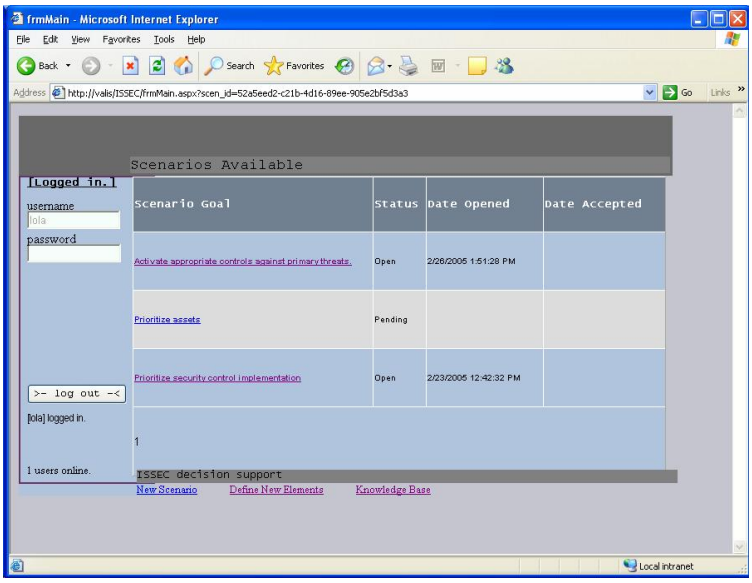

Figure 5. ISSEC-DSS: Scenarios in progress, user view.

Selecting the scenario ("Prioritize security control implementation"), entering the scenario view, the user elects to run the scenario and begins the pair-wise comparison process (which in this scenario will involve 12 comparisons). As seen in Figure 6, this user is strongly favoring "Prevention" over "Purchase Cost".

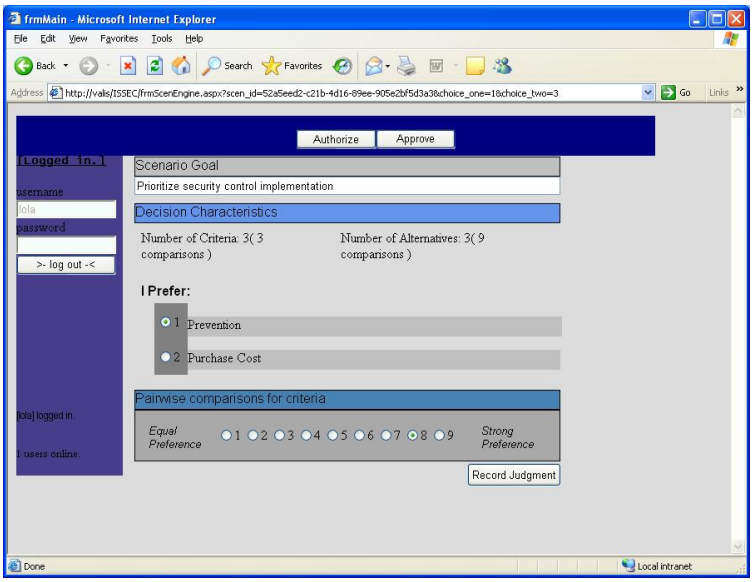

Figure 5. ISSEC-DSS: Scenario preference gathering.

Our user completes the comparisons of criteria, and then ranks the alternatives against one another with respect to each criterion (not shown). Having completed these judgments, the user is able to view the resulting criteria preferences as well as a prioritized ranking of alternatives (Figure 6). Based on the preferences (favoring of "Prevention" ability [67.5%] significantly above both "Purchase Cost", a number which is obviously much higher for the firewall than either a policy change or a free Open Source IDS solution, and "Detection" ability [6.54%]), the system recommends the firewall, despite the fact that it is much more costly.

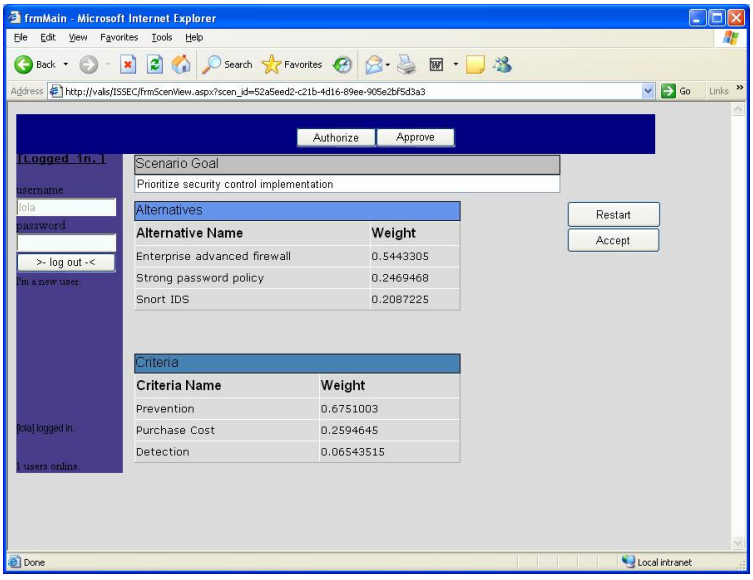

Figure 6. ISSEC-DSS: Scenario results for an individual user.

The user agrees with the results (otherwise, the process can be repeated), and so opts to "Accept" the results, and the hierarchy is persisted to the data warehouse. At this point, to show the aggregate, we assume that the other users follow a similar process of judgment taking. After this is accomplished, the scenario creator enters the Group results panel (Figure 7)

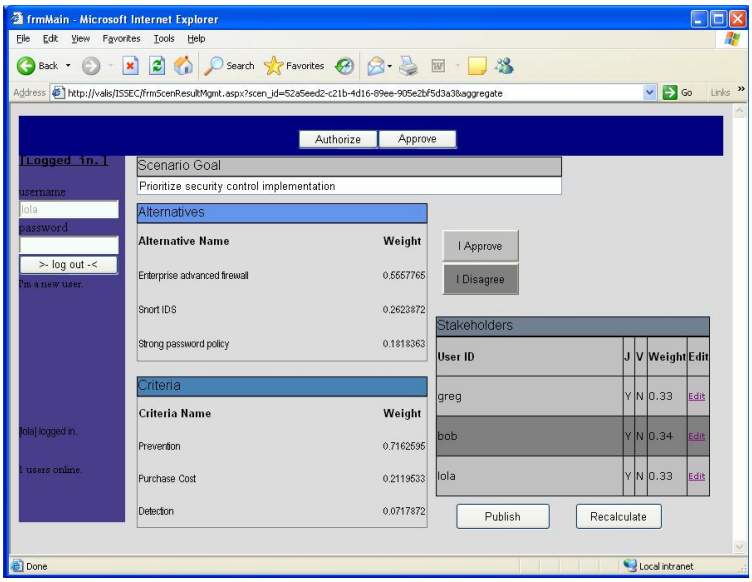

Figure 7. ISSEC-DSS: Scenario results for the group.

The final results from the 'simple democracy' weighting of stakeholders preferences end up fairly similar to those of our individual user. "Prevention" is highly favored (71.6%), which tips the scales in favor of the firewall solution. It also indicates to the decision-maker, however, two important facts: "Purchase Cost" remains an important consideration (21.2%) and the interest in Detection solutions is quite negligible. This console shows the scenario designer the status of this scenario (all stakeholders have provided their judgments and none have voted on the outcome. The scenario designer opts to "publish" the results, which means that each group member can now view the aggregate total and vote on the outcome.

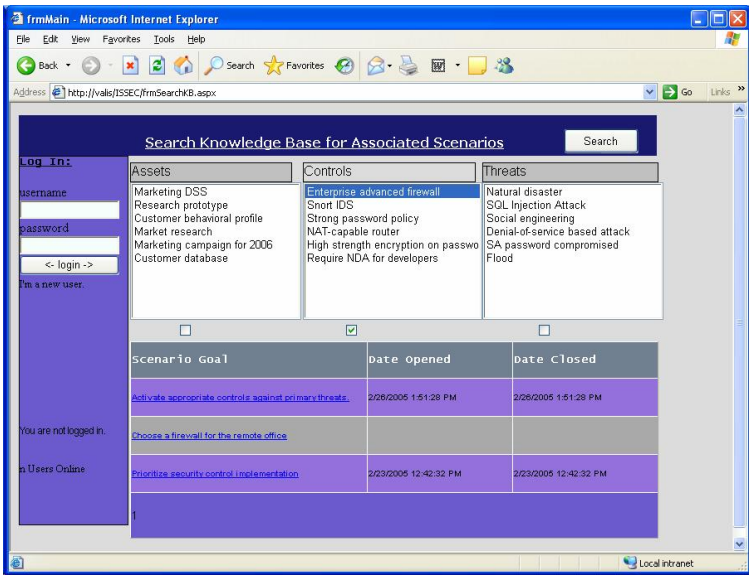

Figure 8. ISSEC-DSS: Searchable knowledge base

Having completed the process, the archived results are now available through a searchable knowledge base (Figure 8) to form the basis of new scenarios, or to support future managerial inquiries to gather situational knowledge in regard to various assets, threats, and controls, and useful aggregates are available in the warehouse for future analysis.

RESULTS AND CONCLUSION

The traditional notion of information security, rooted in a solidly technical foundation, has within the past decade seen wide criticism within academia - much of which has originated from the social sciences community - as being narrow and technology-centric instead of holistic and organizational in its focus. As information security awareness encompasses an

ever-greater scope of organizational dynamics, it becomes necessary for us to develop design methodologies and ultimately, systems, capable of dealing practically with the complex and multifaceted nature of the decision-making of information systems security which is entailed by such emerging notions of a "new paradigm" for security, which can begin to address the concerns of the socio-technical school.

Such conceptualizations must eventually be tested through experiment and application in real-world contexts if they are to advance the state of security management. To this end, we developed an initial prototype demonstrating the system architecture, which implements a web-based multi-user DSS for scenario-based multi-criteria decision making. Through the case study, we can see the trade-offs in a decision fairly explicitly through this type of approach. Even with our simplified example, priorities become apparent, which affect the final decision outcome based on user preferences. As a technique for risk assessment, control selection and asset prioritization, 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. The ability to represent these criteria offers advantage over checklist-based and matrix-based approaches and can deal with conflicting priorities. It can be a valid approach in combination with quantitative techniques, used to weight the relative importance of quantitative data relative to other criteria.

Recommendations for future research

We have presented a deliberately idealized framework that implements a socio-technical design approach to security decision-making through MCDM. Obviously there are opportunities to utilize more sophisticated methods of aggregation and variations on AHP and other multiple criteria approaches known in the literature, than we implemented in the prototype system demonstrated here. Exploration of the application of some of these techniques is expected. The initial results are encouraging, but more extensive field application of the system is necessary.

ACKNOWLEDGMENTS

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

REFERENCES

1. Baskerville, R., & Siponen, M. T. (2001). An Information Security Meta-policy for Emergent Organizations. *Journal of Logistic Information Management*(Special Issue on Information Security).
2. Baskerville, R. (1993). Information systems security design methods: Implications for information systems development. *ACM Computing Surveys, 25*(4), 375.
3. Bell, D. E., & LaPadula, L. J. (1976). *Secure computer system: Unified exposition and multics interpretation*: Technical Report MTR-2997, The MITRE Corporation, Bedford, Massachusetts.
4. Bryson, N. (1996). Group decision-making and the analytic hierarchy process: Exploring the consensus-relevant information content. *Computers & Operations Research, 23*(1), 27.
5. Churchman, C. W. (1971). *The Design of Inquiring Systems: Basic Concepts of Systems and Organizations*. New York, NY: Basic Books.
6. Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A model for evaluating IT security investments. *Communications of the ACM, 47*(7), 87.
7. Courtney, R. (1977). *Security risk assessment in electronic data processing.* Proceedings of the AFIPS Conference Proceedings of the National Computer Conference, Arlington, VA.
8. El-Gayar, O. F., & Fritz, B. D. (2004). *A framework for decision support in information systems security*. Proceedings of the The Tenth Americas Conference on Information Systems (AMCIS), New York.
9. Gaskell, G. (2000). *Simplifying the onerous task of writing security policies.* Proceedings of the First Australian Information Security Workshop, Deakin University, Geelang, Victoria.
10. Greenwald, S. J. (1998). *Discussion Topic: What is the old security paradigm?* Proceedings of the Proceedings of the New Security Paradigms Workshop, Charlottesville, Virginia.
11. Hwang, C. L., & Yoon, K. (1981). *Multiple Attribute Decision Making: Methods and Applications.* Berlin, Germany: Springer-Verlag.
12. Jager, P. d. (2004). The myth of technical security. *American Bankers Association. ABA Banking Journal, 96*(1), 8.
13. Kort, P. M., Haunschmied, J. L., & Feichtinger, G. (1999). Optimal firm investment in security*. *Annals of Operations Research, 88*, 81.
14. Lampson, B. W. (1971). *Protection.* Proceedings of the Proceedings of the 5th Princeton Symposium on Information

Sciences and Systems, Princeton, New Jersey.
15. Mumford, E. (1996). *Systems Design: Ethical tools for ethical change*: Macmillan Basingstoke.
16. Nunamaker, J. F., Briggs, R. O., & Mittelman, D. R. (1996). *Lessons from a dacade of group support systems research.* Proceedings of the Hawaii International Conference on Systems Science (HICSS), Hawaii.
17. Muralidharan, C., Anantharaman, N., & Deshmukh, S. G. (2002). A multi-criteria group decision making model for supplier rating. *Journal of Supply Chain Management, 38*(4), 22-33.
18. Olson, D. L. (2001). Rationality in Information Systems Support to Decision Making. *Information Systems Frontiers, 3*(2), 239.
19. Power, R. (2002). CSI/FBI Computer Crime and Security Survey. *Computer Security Issues and Trends, 8*(1), 1-24.
20. Rees, J., Bandyopadhyay, S., & Spafford, E. H. (2003). PFIRES: A policy framework for information security. *Communications of the ACM, 46*(7), 101.
21. Richardson, S. M., Courtney, J. F., & Paradice, D. B. (2001). An Assessment of the Singerian Inquiring Organizational Model: Cases from Academia and the Utility Industry. *Information Systems Frontiers, 3*(1), 49.
22. Saaty, T. (1980). *The Analytic Hierarchy Process*. New York: McGraw-Hill.
23. Sena, J. A., & Shani, A. B. (1999). *Intelligence Systems: A sociotechnical systems perspectives.* Proceedings of the ACM SIGCPR conference, New Orleans, LA.
24. Senge, P., & Sterman, J. (1992). Systems thinking and organizational learning: Acting locally and thinking globally in the organization of the future. *European Journal of Operational Research, 59*(1), 137-150.
25. Simon , H. (1960). *The new science of management decision*. New York, NY: Harper and Brothers.
26. Siponen, M. T. (2001). Five dimensions of information security awareness. *ACM SIGCAS Computers and Society, 31*(2), 24-29.
27. Smedinghoff, T. J. (2005). Trends in the Law of Information Security. *Intellectual Property & Technology Law Journal, 17*(1), 1.
28. Stein, E., & Zwass , S., V. (1995). Actualizing organizational memory with information systems. *Information Systems Research, 6*(2), 85-117.
29. Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441.
30. Tavana, M. (2003). CROSS: A multicriteria group-decision-making model for evaluating and prioritizing advanced-technology projects at NASA. *Interfaces, 33*(3), 40.
31. Vargas, L. G. (1990). An overview of the Analytic Hierarchy Process and its applications. *European Journal of Operational Research, 48*, 2-8.
32. Whitman, M. E. (2003). Enemy at the gate: Threats to information security. *Communications of the ACM, 46*(8), 91.
33. Willison, R., & Backhouse, J. (2003). *Understanding Criminal Opportunity in the IS Context.* Proceedings of the IRIS, Finland.
34. Vihakapirom, P., & Li, K. (2003). *A framework for distributed group multi-criteria decision support systems.*, from http://ausweb.scu.edu.au/aw03/papers/li/paper.html