Association for Information Systems
AIS Electronic Library (AISeL)

UK Academy for Information Systems Conference Proceedings 2015

UK Academy for Information Systems

Spring 4-1-2015

Multi-Objective Decision Model for Information Systems Risk

Sergio Nunes
ISEG, Portugal, snunes@advance.iseg.ulisboa.pt

Gupreet Dhillon
VCU, United States of America, gdhillon@vcu.edu

Mario Caldeira
ISEG, Portugal, caldeira@iseg.ulisboa.pt

Multi-Objective Decision Model for Information Systems Risk

Sérgio Nunes
ISEG-School of Economics and Management, University of Lisbon, Portugal
Email: snunes@advance.iseg.ulisboa.pt

Gurpreet Dhillon
Virginia Commonwealth University,USA

Mário Caldeira
ISEG-School of Economics and Management, University of Lisbon, Portugal

Abstract

This short paper details research in progress that presents a Multi-Objective Decision Model for assessing Information Systems Risks. The decision model is based on the values and perceptions of stakeholders. It uses the Value-Focused Thinking approach, as opposed to the predominant Alternative-Focused Thinking. The objectives serve as a basis for decision making in the context of Information Systems risk management in complex managerial situations. In this paper the methodology used is presented, discussed and illustrated and a multi-objective decision model for Information Systems risks is developed.

Keywords: IS Risks, Value-Focused Thinking, Multi-Objective Decision Model

1.0 Introduction

The technological and regulatory environment of organizations is becoming increasingly complex. Basel II and SOX require companies to undertake periodic risk assessments. However, Information Systems (IS) risk assessment is a moving target, largely on account of the inherent complexity of infrastructures and technological interdependencies. Compliance with regulatory requirements usually results in a "checklist" approach to managing risks. In such cases, a predetermined list of identified risks is made, and any assessment typically checks whether certain requirements have been fulfilled, or not. Such practices have typically been critiqued in the literature, and their limitations are highlighted (Dhillon and Backhouse, 2001).

It is therefore important to consider how IS risks can be understood and prioritised and to take appropriate decisions. Rather than focus on alternatives, Keeney (1992) argues the usefulness and relevance of value-focused thinking. Keeney notes that alternative-focused thinking limits decision criteria by focusing only on the alternatives, rather than concentrating on companies' objectives, which are driven by

values. The correct approach is that of value-focused thinking, whereby values are linked to alternatives for achieving them, thus identifying better decision-making situations, which consequently turn a reactive decision process into a proactive one (Keeney, 1996).

This research in progress details a Multi-Objective Decision Analysis of Information Systems Risk, using a value-focused approach, with the ultimate goal of helping information systems managers with the decision process for mitigating risks.

2.0 Recent research using VFT in Information Systems

This section details recent research of value-focused thinking (VFT) applied to Information Systems. Barclay and Osei-Bryson (2008) present the Project Objectives Measurement Model (POMM), using value-focused thinking and Goal Question Metric (GQM) techniques. They explain that "POMM involves the elicitation of objectives and measures that reflect the strategic and tactical vision of the project from the perspectives of its multiple stakeholders". They verify the applicability of POMM with two rounds of interviews with subject matter specialists. The first round involved the gathering of perspectives regarding the model, whilst the second focused on discussing specific points for improvement. They present a practical illustration of POMM on programme design within a graduate programme at a university, thesis development and also thesis outcome evaluation. They develop a means and fundamental objectives network and also develop metrics to monitor and evaluate the degree of achievement of fundamental objectives. In Barclay and Osei-Bryson (2009), the authors apply POMM to a different project in a large financial services company, and evaluate the average priority of objectives collected, using value-focused thinking. The project consisted of automating a decision support information system to substitute multiple reports that were previously being compiled manually.

Barclay and Logan (2013) integrate stakeholders' values to enhance the implementation, adoption and delivery of a large scale online open access course (MOOC), using a value-focused approach. The study takes place at a university in the Caribbean, with the collaboration of teachers, students, administrative staff, online learning specialists, and education executives. The results include multiple means objectives that led to establishing 5 fundamental objectives, namely: maximise preparedness for the professional world, maximise satisfaction with the learning

experience, maximise viability of MOOC offering, maximise access to learning, and maintain reputation for quality.

Dhillon and Chowdhuri (2013) collected individual values for protecting identity in social networks, using a value-focused thinking mind-set. They interviewed 147 individuals and summarised social media objectives across 19 clusters, divided into 5 fundamental objectives, and 14 means objectives. The 5 fundamental objectives are: maximise end-user trust, ensure development of social networking ethics, ensure authentication of user identity, maximise identity management to make social networks useful, and, maximise social networking infrastructure protection. These results deliver a roadmap that individuals and organisations can use to set up an identity protection strategy for social networks.

May et al. (2013) define value-based objectives for the planning of Enterprise Resource Planning (ERP) systems. They defend that there is commonly a misalignment between organizational business processes and ERP packages. In order to narrow this gap, they use value-focused thinking to develop a list of objectives collected through 16 interviews across 3 ERP implementation case studies in Southern Europe. They argue that, by omitting to determine stakeholder values prior to the implementation of ERP, a project will only consider the technical implementation as being the main critical success factor, at the same time disregarding other social, organizational and contextual factors. The results consisted of 13 means objectives and 4 fundamental objectives, namely: minimise cost, ensure ERP benefits realization, enhance product and service improvement and maximise customer relationship effectiveness. Tying these objectives to stakeholder values helps organizations understand better the complex technical and social issues that are related to ERP projects, and provides the basis for developing an ERP strategic plan.

3.0 Methodology

In this section we present the methodology employed to define a multi-objective decision analysis model for information systems risk. We developed our research methodological process (Figure 1) by taking into account the work by Keeney (1992) and Shoviak (2001). The first and second steps have already been completed by the authors. The remaining steps are in progress.

3.1 Enumerate values and identify objectives

The values for risk management were gathered by conducting semi-structured interviews with several security and IT professionals. A total of 71 interviews were conducted, and a total of 612 risk management values were collected, and after removing duplicates, a total of 414 values were identified. The values in a common form were then transformed into 114 distinct objectives, and any duplicates were then removed, which resulted in the same goal, but expressed in different words, following on from a correlation and consolidation procedure.

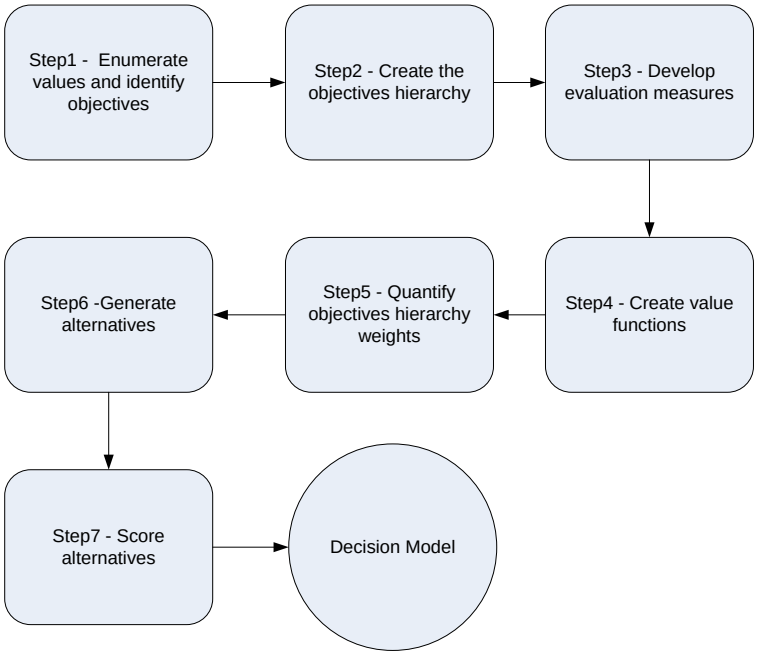

Figure 1. Research Methodological Process

3.2 Create the objectives hierarchy

Keeney (1988) describes that the structuring of objectives into a hierarchy improves communication among stakeholders, thus creating a basis for the common understanding of values, which leads to compromise as a means of achieving consensus. The communication barrier that arises from the use of specific language can separates multiple specialities, such as IT for example, and the business then becomes minimised by the common understanding of values. The early involvement of stakeholders in the decision process increases their willingness to cooperate in achieving a common goal.

In this step, the objectives were sorted into 23 clusters, taking into account a shared common theme. These 23 clustered objectives were further classified into means and fundamental objectives, by using the "why is this important" (WITI) test. This structured procedure is important for enabling reflection as to what individuals care about with regards to risk, and also for seeing how these objectives rank in terms of importance. The WITI test resulted in a total of 6 fundamental objectives, and 17 means objectives, as can be seen in Table 1.

Overall objective: Minimise IS risks	
Means Objective	**Fundamental Objective**
-Ensure properly configured IT infrastructure -Promote IS risk performance metrics -Ensure ongoing monitoring of IS risks -Ensure IS risk management processes are audited -Maximise access control -Minimise IS risks related to IT service providers -Reduce human negligence -Maximise vetting of employees for IS risks -Ensure adequate internal communication regarding IS risks -Ensure adequate external communication regarding IS risks -Maximise IS risks management for critical information -Ensure information confidentiality -Ensure information availability -Ensure information integrity -Develop IS risk management competencies -Develop an IS risk awareness programme -Develop a training programme for IS risk management	-Ensure risk management governance -Maximise IS risk knowledge -Ensure IS security quality -Maximise responsibility and accountability for IS risks -Maximise compliance -Maximise the protection of human life

Table 1. Means and fundamental objectives for IS risk management

3.3 Develop evaluation measures

Attributes that measure the achievement of defined objectives are divided into 3 types (Keeney and Gregory, 2005): natural, constructed and proxy attributes. The natural attributes are intuitive by nature, an example being that the number of fatalities per time frame is an attribute of the objective of setting automotive speed limits. The proxy attribute is characterised by not measuring the objective directly, but instead by counting it in conjunction with other attributes to define whether the objective has

been achieved. Using the same example of setting a speed limit, the proxy attribute for an example can be the number of accidents. The constructed attributes are, as its name implies, the construction of a scale whereby the natural attribute does not exist. Once the scale is known and is continuously in use, the constructed attribute then becomes intuitive and resembles a natural attribute. Proxy attributes are most used when an intuitive natural attribute lacks information, and they thus apply to means objectives which influence the achievement of the basic objective.

In the IS risk context, if we take as an example - the means objective of "Develop a training programme for IS risk management", then an attribute that needs to be measured could be the "Number of people trained in IS risk management per year".

3.4 Create value functions

The measures in the previous step can be a mixture of different measurement units and different scales, thus we need to unify all measures into one common value function, which is situated between 0 and 1. Taking into account the previous example of "Develop a training programme for IS risk management", with the attribute "Number of people trained in IS risk management per year", we surmise that in this case, the decision maker might well postulate whether he wants at least 50 people to be trained per year, which would lead to 50 people or more being attributed the value 1. If 0 people were trained, then a value 0 would be attributed, as can be seen in Figure 2.

Figure 2. Value function

3.5 Quantify objectives hierarchy weights

The objectives will be weighted using the swing method (Kirkwood, 1997), whereby a panel of specialists in risk management is asked to judge the importance of

objectives designed for the global objective of minimising risk for information systems. This approach leads to attributing a local weighting to each sub-objective in a branch. All the local weightings in a branch will sum up to 1, in order to fulfil the main objective. A multi-tier hierarchy is then evaluated with global weightings, whereby local weightings are multiplied to accomplish the main objective, using an additive function. In the example in Figure 3, the global weightings are placed in, whilst brackets are not used for local weightings.

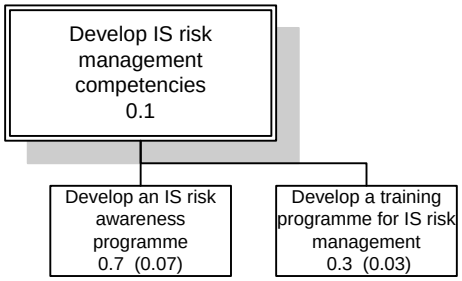

Figure 3. Local and global weightings

3.6 Generate alternatives

In addition to the initial alternatives that were the basis of the decision analysis using value-focused thinking, the ongoing research will discover other hidden alternatives among stakeholders as a result of discussing the value-focused thinking process, along with the attributes and weightings agreed for the objectives.

This dismembering of the decision process is achieved by using value-focused thinking, which allows for the removal of psychological traps which influence our clear judgment about creating new alternatives, without being limited to the previous alternatives (Keeney, 2004).

3.7 Score alternatives

All alternatives will be ranked by taking into account the fulfilment of all the objectives. The best alternative can be far removed from the theoretically ideal solution which maximises all objectives. Nonetheless, it is possible to evaluate the gap between the best-scored alternative and the ideal solution. This gap allows decision makers to consider changing some of the characteristics of the best scored solution, in order to increase the matching with the theoretically ideal solution.

4.0 Conclusion

This paper presents research in progress that seeks to create a multiple objective decision analysis model for minimising risk for information systems. It uses the value-focused thinking methodology conceived by Keeney (1992) for the creation of objectives derived from IS risk values, and this also serves as a basis for helping information system managers decide on the best alternatives for mitigating risk.

References

Barclay, C. and Logan D. (2013), *Towards an Understanding of the Implementation & Adoption of Massive Online Open Courses (MOOCs) in a Developing Economy Context*. Proceedings of SIG GlobDev Sixth Annual Workshop, Milano, Italy.

Barclay, C. and Osei-Bryson K.-M. (2008), *The project objectives measurement model (POMM): An alternative view to information systems project measurement.* Electronic Journal of Information Systems Evaluation 11(3), 139–154.

Barclay, C. and Osei-Bryson K.-M. (2009), *Determining the contribution of IS projects: an approach to measure performance*. In: System Sciences. HICSS'09. 42nd Hawaii International Conference on. pp. 1–10.

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

Dhillon, G. and Chowdhuri R. (2013), *Individual values for protecting identity in social networks*. Thirty Fourth International Conference on Information Systems, Milan.

Keeney, R. L. (1988), *Structuring objectives for problems of public interest*. Operations Research 36(3), 396–405.

Keeney, R. L. (1992), *Value-Focused Thinking: A Path to Creative Decisionmaking*. Harvard University Press.

Keeney, R. L. (1996), *Value-focused thinking: Identifying decision opportunities and creating alternatives*. European Journal of Operational Research 92(3), 537–549.

Keeney, R. L. (2004), *Making better decision makers*. Decision Analysis 1(4), 193–204.

Keeney, R. L. and Gregory R. S. (2005), *Selecting attributes to measure the achievement of objectives*. Operations Research 53(1), 1–11.

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

May, J., Dhillon G., and Caldeira M. (2013), *Defining value-based objectives for ERP systems planning*. Decision Support Systems 55(1), 98–109.

Shoviak, M. J. (2001), *Decision Analysis Methodology to Evaluate Integrated Solid Waste Management Alternatives for a Remote Alaskan Air Station*. Wright-Patterson Air Force Base, Ohio: Air Force Institute of Technology.