Value Focused Approach to Information Systems Risk Management

Sérgio Nunes, University of Lisbon, Portugal, snunes@advance.iseg.ulisboa.pt
Gurpreet Dhillon, Virginia CommonWealth University, USA, gdhillon@vcu.edu
Mário Caldeira, University of Lisbon, Portugal, caldeira@iseg.ulisboa.pt

Abstract

Information Systems (IS) risk management is a challenge to every organization, in that they are exposed to cyber-attacks that bypass physical barriers. Organizations increase online business in order to remain competitive, but as a consequence their online exposure becomes greater. However their risk management practices and governance are inadequate in the face of increasing new threats and vulnerabilities. This paper 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.

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

1. INTRODUCTION

Nowadays most enterprises have requirements to protect the information security from outsiders, competitors and even between employees from different departments. It has been proven that disgruntled employees are seen as a massive threat to information security as they have access to sensitive information that can put the company's reputation at stake, although they are frequently perceived by management as trusted personnel that follow safeguards [Dhillon, 2001]. The enforcing of regulatory requirements like Basel II or SOX by supervision entities force enterprises to conduct information systems risk assessments and perform strict management of information security.

Top management recognizes the need of information security, but how much of information security investment is enough? An information security budget is seen by top management as a black hole that sucks resources and investment without any returns. What are the return benefits of security investments? Although the information security manager is fighting daily to align business objectives with security objectives, it is not always possible to achieve a direct alignment between them. A key factor in influencing top management to expand the information security budget is risk.

Risk is the common language between information security and the business, by translating the technical details into business losses and bringing top management long term commitment to the security strategy

ISSN 2183-489X
DOI http://dx.doi.org/10.18803/capsi.v15.103-115

[Vitale, 1986]. Security investments, most of the times, do not bring tangible added value to business, but they mitigate risk to an acceptable level by management by following a cost benefit approach. The security budget lives from those detected risks, based on the importance of the critical business assets that it protects. Information systems entail complex technological environments and are targeted by multiple threats with a probability of being exploited. A successful exploitation of a vulnerability in the information systems might expose critical business information. Top management is flooded with multiple risks and are urged by stakeholders to decide on the best alternative as soon as possible. Should the decision be focused in an alternative based approach?

[Keeney 1992] argues that alternative focused thinking limits the decision criteria by focusing only on the alternatives rather that concentrating on company's objectives that are driven by values. Alternatives are pushed by others to force a decision among measures that are not aligned with business objectives and can result on the least damaging alternative being chosen by top management without appropriate reflection on business values. Values should drive decision making as they drive intrinsically everything we do. Deciding on alternatives without understanding the values behind them and without matching the alternatives towards company's values will constrain the decision process. The right approach is a value focused thinking where values articulate different alternatives that achieve them, thus identifying better decision situations and changing a reactive decision process into a proactive process [Keeney, 1996].

2. LITERATURE REVIEW

The literature review process started by looking at research that employed the value focused thinking in multiple areas namely energy, information systems (IS), information security and operations [Parnell et al., 2013]. The problem always resides in the ability to justify a difficult decision by weighting the multiple objectives [Keeney et al., 1986].

[Dhillon and Torkzadeh 2006] present an assessment of information systems security in organizations, in which they use a value focused approach with the major objective of maximizing information systems security in organizations. They interviewed 103 managers from multiple organizations and initially identified general values for managing information systems security and recorded them in a wishlist. In a second phase values are clustered, labeled and converted into security objectives. The third phase consists of the classification of the objectives in the fundamental and means objective group by elaborating the "why is it important?" (WITI) test. The final phase deals with the validation of the objectives list in a panel of experts. The research resulted in 86 objectives that were organized into 25 clusters with 9 fundamental and 16 means objectives. According to the authors a need to amplify the principles beyond confidentiality, integrity and availability arises for designing security, as other objectives were valued by the employees.

[Duarte and Reis 2006] use the VFT approach and the multiple attribute value theory to gather the objectives to help the Portuguese Public Administration to choose among projects implementation. The objectives considered are: ”maximize the innovation, maximize the geographical impact (economics of scale), maximize the connection between partners and skills (networking effect), maximize the number of direct beneficiaries (Enterprises, Citizens and other Organizations), maximize the number of agents indirectly benefited (Enterprises, Citizens and other Organizations), maximize the technical skills of employment (jobs created and maintained), maximize the economic efficiency (economic sustainability) and maximize the synergies between actions (project integration)”. The second step consisted of developing multiple attributes from the objectives to be able to weight projects and support decision making. They tested the evaluation framework against 5 project proposals, where 2 projects were terminated after evaluation, and developed a computer interface to be able to apply the same principle to other future project proposals in a simplified approach.

[Mishra and Dhillon 2008] develop control objectives based on the values of IT managers using a value focused approach. They classify controls according to scope of control and target of control. In scope of control, controls can be classified as technical, formal and informal. Technical controls target electronic information and can be for example the use of encryption algorithms or authorization mechanisms. Formal controls target organizational structure and management and an example is the enforcement of policies, standards and procedures. Informal controls deal with the importance of values and examples are the expectations of responsibility and accountability. The target of control can be input, behavioral and output. Input controls deal with the alignment of employees with business interest by applying training programs. Behavioral controls determine how work is accomplished in the organization through the following of defined business processes. Output controls manage results by measuring the transformation process. With this classification process in mind they interviewed 54 individuals and gathered 7 fundamental objectives and 18 means objectives related to internal controls. By analyzing the outputs they conclude that technical controls by themselves cannot provide the necessary information security governance that an organization needs. They state that a formal control structure should be present in the organization by enforcing documented policies and procedures via top-down approach with top management awareness and involvement. Informal values should not be underestimated by the business as they enhance the impact of security governance and motivate employees, if the business and individual values are aligned to achieve a sense of ownership, ethical behavior and trust.

[Averill et al. 2009] discuss egress technology, efficient communication and safe evacuation during emergencies from large buildings using a VFT approach during a 3 day workshop. They gathered 7 main objectives: save lives and prevent injuries to occupants, save lives and prevent injuries to firefighters/responders, minimize property damage, minimize impact on property operations, minimize economic costs, reduce stress and reduce grief. The discovery of alternatives to respond to the multiple objectives is also a goal of the workshop, so it was divided into 2 stages. The first stage entails the

individual definition of values and their objectives along with the alternatives to achieve those objectives. The second phase includes the group discussion of the proposed objectives and alternatives and the creation of multiple subgroups to reevaluate and discover new alternatives. The alternatives were classified on 3 criteria: quality, feasibility and creativity. Quality deals with effectiveness of the alternative, feasibility concerns the implementation within a 10 year period and creativity awards out of the box ideas.

[Dhillon and Chowdhuri 2013] collect individual values for protecting identity in social networks using a value focuses thinking mindset. They interviewed 147 individuals and summarized social media objectives across 19 clusters divided by 5 fundamental and 14 means objectives. The 5 fundamental objectives are: maximize end user trust, ensure development of social networking ethics, ensure authenticity of user identity, maximize identity management to make social networks useful and maximize social networking infrastructure protection. These results deliver a roadmap for individuals and organizations to be able to set up an identity protection strategy for social networks.

[May et al. 2013] define value-based objectives for Enterprise Resource Planning (ERP) systems planning. They defend there is commonly a misalignment between organizational business processes and ERP packages. To narrow this gap they use value focused thinking to develop a list of objectives collected with 16 interviews across 3 ERP implementation case studies on Southern Europe. They argue that without determining stakeholders values prior to the ERP implementation, the project will only consider the technical implementation as the main critical success factor, disregarding other social, organizational and contextual factors. The results consisted of 13 means objectives and 4 fundamental objectives: minimize cost, ensure ERP benefits realization, enhance product and service improvement and maximize costumer relationship effectiveness.

These objectives grounded in stakeholders values aid organizations to understand the complex technical and social issues related to ERP projects and provide the basis to develop an ERP strategic plan.

3. METHODOLOGICAL APPROACH

The basis of this research is value theory [Catton, 1954, 1959] and the method employed is the value focused thinking approach [Keeney 1992]. [Catton 1959] explains that valuing is defined by the intensity of the desire to obtain an object and that the preference follows a motivational pattern. [Catton 1959] defines value as: ”a conception of the desirable which is implied by a set of preferential responses to symbolic desiderata”. He states that value conceptions are “socially acquired”. He explains that some researchers advocate that values cannot be measured, but he argues that by following a judgment based on values it is possible to make predictions of decisions in a defined context. These values guide the decision makers in a decision analysis process. [Keeney 2004] defines decisions: ”as situations where the decision maker recognizes that a conscious choice can be made”. The ultimate goal by following value focused thinking in decision analysis

should be to select the best alternative, but as that is not always possible due to hidden alternatives. The enumeration of values and the creation of objectives serve the principle of eliminating the bad decisions that looked good before, but do not accomplish any of the proposed objectives. The unframing of the decision process should be performed as soon as possible by defining the problem at hand and removing the psychological traps that influence our clear judgment in creating new alternatives without the anchoring in the previous alternatives.

[Keeney 1992] explains that values are principles for evaluation of the consequences of action or inaction towards a decision among different alternatives. He enumerates the uses of value focused thinking: ”uncovering hidden objectives, guiding information collection, improving communication, facilitating involvement in multiple stakeholder decisions, interconnecting decisions, evaluating alternatives, creating alternatives, identifying decision opportunities and guiding strategic thinking”.

[Gregory and Keeney 1994] argue that value focused thinking is a facilitator in a negotiation situation to reach consensus among stakeholders, as the unique list of objectives is part of the values and contributions from all the people involved in the decision process. This list of objectives forms the context to evaluate alternatives that assure the commitment from stakeholders, even if each stakeholder wants to push an alternative, he will have to justify the inclusion of the alternative as a consequence of multiple previous agreed objectives. The design of alternatives will have also to take into account the accomplishment of the type of objective, namely the division between fundamental and means objective.

[Keeney and Gregory 2005] research the process of the creation and selection of attributes that measure the achievement of the defined objectives of value focused thinking. They describe 3 types of attributes: natural, constructed and proxy attributes. The natural attributes are intuitive in nature, in which for example the number of fatalities per time frame is an attribute to the objective of setting automotive speed limits. The proxy attribute is characterized by not measuring the objective directly, but count in conjunction with other attribute to define the objective’s achievement. Using the same example of setting the speed limit, the proxy attribute can be for example the number of accidents. The constructed attributes, are like the name explains, the construction of a scale when the natural attribute doesn’t exist. Once the scale is known and continuously used, the constructed attribute becomes intuitive and resembles a natural attribute. Proxy attributes are most used when the intuitive natural attribute lacks information, so they apply to means objectives that influence achievement of the fundamental objective.

The combination of the different attributes into a value model follow 3 main independence concepts [Keeney 2001]: additive, preferential and utility independence. Additive independence means that the attributes do not escalate taking into account the consequences of the objective, for example saving money on product 1 and saving money on product 2 can be added to fulfill the objective saving money on products. Preferential independence deals with pairs of attributes that are independent from the other attributes. Utility independence

normally involves risk situations where the risk taking strategy from one attribute is independent from the fixed levels of other attributes. These independence concepts lead to 2 value model alternatives. The additive value model functions when all attributes are additive independent and the multiplicative value model functions when each pair of attributes is preferential independent and one attribute is utility independent. The common uses of value models are the creation of alternatives, evaluating existing alternatives, product design, guiding information collection, identifying and resolving conflicts, facilitating decision making, and identifying decision opportunities.

Adapting the approach from [Keeney 1992] and [Shoviak 2001], the research process can be summarized into a 5 step methodology:

1. Collect the detailed list of values for the decision context;
2. Rewriting the values in a common form, transforming them into sub objectives and clustering them into main objectives;
3. The clustered objectives are classified into fundamental objectives and means objectives, using the "why it this important" (WITI) test;
4. Weight the fundamental objectives;
5. Develop attributes to measure the objectives.

4. VALUE FOCUSED IS RISK MANAGEMENT

The initial list of values for IS risk management were gathered by conducting semi structured interviews in Portugal with several security and IT professionals who represented a wide variety of job descriptions, such as the CIO, CISO or IT Manager, for example. The interviewees were representative of multiple business sectors, but were predominantly from consultancy, banking and the telecommunications industry. Should the information gathered require further explanation that was relevant for the research, we interviewed other employees from the same organization in order to clearly identify the context of the information collected. The interview data gathering approach is adequate, as values should not be constrained and should be intrinsic from the individual. Interviews were conducted within borders by using general targeted topics, broad categories and examples, but open questions were posed which allowed the respondents to reflect on their past decisions and enabled a review of their judgmental values. A total of 71 interviews were performed. No more were carried out because the total of values that were collected from the last interviews were repetitions of previous values, so we thus opted for theoretical saturation. A total of 612 IS risk management values were collected, and after the removal of duplicates, a total of 414 values were identified. These values were enlisted in a common form and followed the methodology of obtaining a wishlist from the interviewees. The values in a common form were then transformed into 114 distinct sub-objectives, and any duplicates were removed,

which resulted in the same goal in different words, following a correlation and consolidation procedure. This transformation into sub-objectives is accomplished by applying an active verb which turns an objective into an effective action. These objectives were then 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 in a IS risk context, and for seeing how these objectives relate 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.

Means Objectives	**Fundamental Objectives**
-Ensure properly configured IT infrastructure -Promote IS risk performance metrics -Ensure ongoing monitoring of IS risks -Ensure IS risk management processes are audited -Maximize access control -Minimize IS risks related to IT service providers -Reduce human negligence -Maximize vetting of employees for IS risks -Ensure adequate internal communication regarding IS risks -Ensure adequate external communication regarding IS risks -Maximize 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 -Maximize IS risk knowledge -Ensure IS security quality -Maximize responsibility and accountability for IS risks -Maximize compliance -Maximize the protection of human life

Table 1. Means and fundamental objectives for IS risk management

The objectives were weighted using the swing method (Kirkwood, 1997), whereby a panel of specialists in risk management and information security is asked to judge the importance of objectives designed for the

global objective of minimizing risk in information systems. This approach leads to defining a local weighting to each sub-objective in a branch. All the local weightings in a branch 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. For the purpose of weighting the fundamental objectives, we arranged a workshop to foment the discussion and collect the opinion of the attendees regarding the importance of each objective within the model. The workshop was performed within an information security conference with the duration of 40 minutes. There were 31 participants with positions such as for example CISO, IT Manager, Auditor and Professor. We opted to weigh also the 3 basic pillars of information security (information confidentiality, integrity and availability) although they are considered in this model means objectives to accomplish the fundamental objective of ensuring IS security quality, because of their importance in minimizing specific risks inside information systems. The hierarchical model and the local weights are presented in Figure 1.

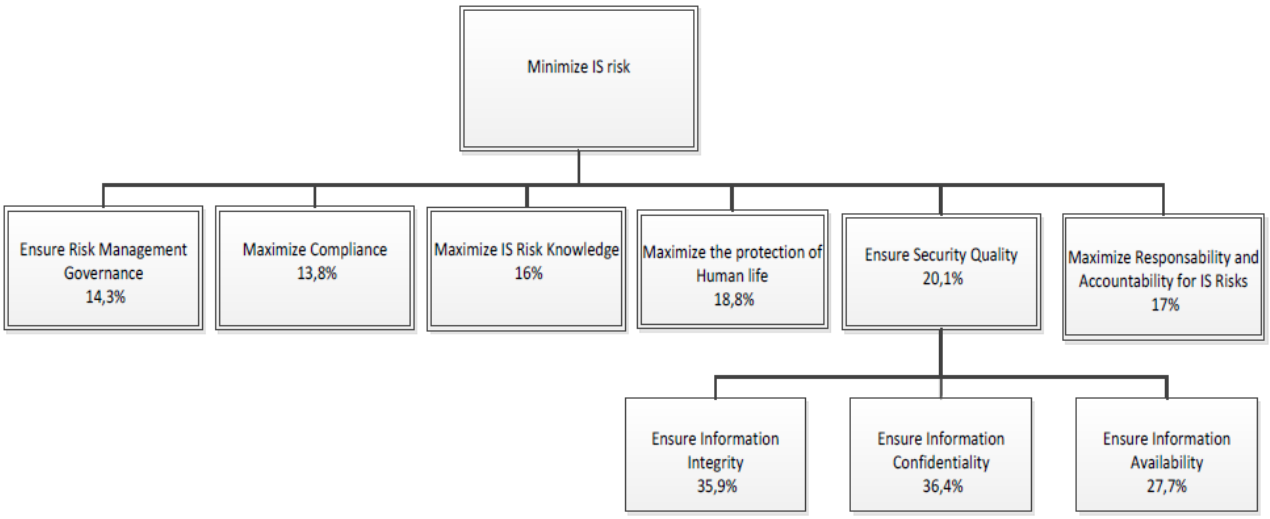

Figure 1 – Hierarchy of objectives

The next step would be to develop attributes to measure the performance of each objective within the model and transform these objectives into value functions that are situated between 0 and 1 to unify the measurement scales.

In the IS risk context, if we take as an example - the objective of "Maximize Compliance", then an attribute that needs to be measured could be the "Number of non-compliance issues per year". This is decreasing value function in which the target is 0 non-compliance issues per year for a value of 1.

5. DISCUSSION

This section discusses each of the 6 IS risk management fundamental objectives and the 3 means objectives present in the model, taking into account existing best practices and by detailing the context in which they were structured and scored.

Ensure risk management governance includes the adoption of IT and security best practices. Adequate risk management governance entails the nomination of a IS risk committee, which has the role of discussing IS risk at top management level and which consults all relevant stakeholders. The weight of this objective in the hierarchy is classified with 14,3% in the overall model which reflects the lack of risk governance maturity in most organizations in Portugal.

Maximize responsibility and accountability for IS risks deals with who does what, and who is ultimately responsible for risk mitigation measures. Most of the time, the person who is responsible for executing tasks is responsible for a specific delegated task, and the data owner is the person who is accountable for either accepting the risk, or deciding whether to implement additional safeguards. These data owners should be clearly identified in IS risk management and, together with their responsibilities in the risk management process, their role should be clear and objective. This identification and definition process prevents finger-pointing across the organization when a risk turns into a real situation. In the model this objective is weighted with 17% which demonstrates the need to assure adequate responsibility and accountability practices.

Maximize IS risk knowledge entails the creation of an intangible capability as a risk management organizational culture, in which each stakeholder is aware of existing IS risks and their management practices. Adequate testing of procedures and know-how should be performed in order to ensure that every employee is informed about the IS risk culture and knows what their role is in that risk management framework. In our model this objective represents 16% of the overall weight and it demonstrates that people skills in risk management are an important objective, but often left in the background in current organizations, as there are always more critical objectives appearing in risk management that need immediate attention.

Maximize compliance deals with ensuring that requirements from supervisory entities are met. This objective impacts on an organization's business directly, as sanctions are applied for lack of compliance and, in extreme cases, this may lead to the legal prosecution of management. An organization has to adopt those proven methodologies, frameworks and best practices that guarantee the maximization of compliance. Risk management has defined standards and best practices which should be adapted for IS risk management in the context of every organization. The documentation of clear IS risk policies and procedures, together with the definition of internal sanctions for their non-compliance, should be an initial step in establishing the risk management framework. Legal compliance issues should also be accounted for, such as, for example, data retention time frames, which differ for each country. Copyright management is also a compliance requirement which affects not only the software acquired by an organization, but also, for example, a IS attack with the

intention of implanting illegal software. This objective was the least scored objective with 13,8%, this score details the significance of compliance in Portugal as the supervision entities are still benevolent in terms of compliance practices, functioning still as advisory when compared with mandatory requirements.

Maximize the protection of human life may seem an outside objective at first glance when dealing with IS risks. However this objective makes complete sense, after careful examination, and when considered within the mindset of those IS risks which affect critical infrastructures that may harm human life. Critical infrastructures are being attacked daily with advanced persistent threats (APT), with the goal of compromising their infrastructures, examples being energy companies and water management, for example. A recent example was when a computer worm named Stuxnet was created to attack nuclear power plants. These IS risks should be carefully managed as most critical infrastructures, although not directly connected to the Internet, are indirectly exposed to attacks and loss of human life may occur. When reflecting about cyber warfare, wars happen first in the cybersphere before a physical attack occurs. It is easier to attack a country that is rendered blind, through the lack of communications or power, for example. Recently, efforts are being secretly pursued by countries to enhance their IS competitive intelligence. At the individual level with the Internet of Things phenomenon, those risks will affect the common citizen in their houses, in their jobs and directly in their life with the adoption of e-health devices for example. The score of 18,8% details that this objective in risk management is still dormant in our lives at the moment, but it may increase dramatically as examples of human losses turn into a reality with vulnerabilities being exploited in information systems.

Ensure IS security quality objective aggregates security concepts, including explicitly the information confidentiality, integrity and availability triad. Examples of some of the fundamental concepts for assuring IS security quality are: information authenticity, reliability and non-repudiation. The ability to counteract aggressive actions can be ensured by robust authentication, complemented with strong auditing mechanisms and an adequate identity management of multiple stakeholders across multiple platforms, and also by using applications with strong access controls. Maintaining data privacy is also a critical factor for strengthening the quality of IS security. Being the model weighting workshop conducted within an information security conference we would expect that this objective is the most critical within the model. This is what happened with this objective weighting 20,1% of the model. Security practices and mechanisms represent the common safeguards to minimize information systems risks and ensuring security quality is a main concern of every information systems professional.

Ensure information confidentiality to prevent sensitive information being leaked to an unauthorized entity. This can be ensured by adopting adequate encryption measures when dealing with stored information, by encrypting laptops' hard drives or critical databases. Information transmitted can also use network protocols, which ensures that the encryption of data and data leak protection (DLP) mechanisms be implemented to

prevent leakage by disgruntled employees. Implementing an information classification program is also a crucial step for defining information's value and for protecting printed documents. In our model this objective contributes 36,4% as a means objective to ensuring IS security quality, being scored as the most important pillar in the CIA triad. This score reveals the importance of information as competitive advantage in most organizations. The global weight of this objective within the hole model is 7,3%. This global value is obtained by multiplying the local value of the means objective (36,4%) with the value of his parent fundamental objective (20,1%).

Ensure information integrity by adopting good change management practices. Change management allows for the tracking of responsibilities and prevents unauthorized and unprepared changes. Changes should be planned and a rollback plan should be available in case corruption of data occurs. The weight of this objective (35,9%) resembles the importance given to the previous objective "Ensure information confidentiality". The global weight of this objective within the hole model is 7,2%.

Ensure information availability when access to information is required by an entity. The risk of loss of information needs to be minimized, and adequate backup procedures and data recovery methods should be tested periodically. The transportation of backup information offsite should be evaluated in order to protect against disaster. Business continuity and disaster recovery best practices should be adopted by the organization, which should include the definition of recovery times and point objectives. The presence of high availability mechanisms in the infrastructure that supports critical processes is an added protection measure against failures, and protects against denial of service attacks. The score of this means objective is 27,7%, being the least prioritized objective in ensuring IS security quality. This reveals that organizations prefer to have their information systems not accessible, than to have information leakage or data integrity compromises. This result goes in opposite direction as the current trend of cloud computing being adopted by enterprises, where information availability is one of the most important benefits of cloud computing, raising issues in the integrity and confidentiality of information. The global weight of this objective within the hole model is 5,6%.

The value focused assessment of IS risks allows managers to base their decisions on stakeholders values that can be subject to analytical generalization in different cases. Yin (2003) argues along that line, and states that analytical generalization leads to theoretical propositions.

This study details the relationship between different objectives and establishes priorities for IS risk mitigation by dividing means and fundamental objectives. The fundamental objectives are weighted in a multi objective decision model. These risk objectives are focused on technical, procedural and social mechanisms. With these objectives an organization can evaluate what are the critical ones for the current business and which safeguards will minimize the current risk level individually. Summarizing the discussion, this study makes the following major contributions:

- It uses Value Focused Thinking as a proven methodology for the exploratory study of the theme of IS risk management;
- It generates a detailed list of values and proposed objectives, based on their contribution to minimizing IS risk;
- It delivers a qualitative prioritized IS risk management decision model with fundamental and means objectives;
- It allows managers to simplify the decision process by justifying which risk management objectives are being addressed with the chosen safeguard.

6. CONCLUSION

This study presents a value focused assessment of IS risks across different organizations in Portugal and presents an IS risk management decision model. This model is composed of structured and weighted objectives which help management decide and justify investment in safeguards that guarantee the ultimate goal of risk mitigation. These objectives establish a roadmap for strategic planning within IS risk management and promote the involvement of stakeholders in the decision process by leveraging different objectives that may be pertinent to each stakeholder.

REFERENCES

Averill, J. D., R. D. Peacock, R. L. Keeney, and P. D. Gallagher, "Rethinking egress: A vision for the future", Vol. Technical Note 1647. US Department of Commerce, National Institute of Standards and Technology 2009.

Catton, W. R. 'Exploring Techniques for Measuring Human Values'. American Sociological Review 19(1), 1954, 49–55.

Catton, W. R.: 'A theory of value'. American Sociological Review 24(3), 1959, 310–317.

Dhillon, G. "Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns." Computers & Security 20 (2), (2001). 165–172.

Dhillon, G. and G. Torkzadeh "Value-focused assessment of information system security in organizations." Inf. Syst. J. 16 (3), (2006). 293–314.

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

Duarte, B. P. and A. Reis, 'Developing a projects evaluation system based on multiple attribute value theory'. Computers & operations research 33(5), 2006, 1488–1504.

Gregory, R. and R. L. Keeney 'Creating policy alternatives using stakeholder values'.Management Science 40(8), 1994, 1035–1048.

Keeney, R. L., J. F. Lathrop, and A. Sicherman 'An Analysis of Baltimore Gas and Electric Company's Technology Choice'. Operations Research 34(1), 1986, 18–39.

Keeney, R. L. "Structuring objectives for problems of public interest." Operations Research 36 (3), (1988) 396–405. ISSN: 0030-364X.

Keeney, R. L. "Value-Focused Thinking: A Path to Creative Decisionmaking". Harvard University Press. (1992) ISBN: 9780674931985.

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

Keeney, R. L. 'Modeling values for telecommunications management'. Engineering Management, IEEE Transactions on 48(3), 2001, 370–379.

Keeney, R. L. "Making better decision makers." Decision Analysis 1 (4), (2004), 193–204. Keeney, R.L. and R. S. Gregory 'Selecting attributes to measure the achievement of objectives'. Operations Research 53(1), 2005, 1–11.

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

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

Mishra, S. and G. Dhillon "Defining Internal Control Objectives for Information Systems Security: A Value Focused Assessment." In: ECIS, (2008). pp. 1334–1345.

Parnell, G. S., D. W. Hughes, R. C. Burk, P. J. Driscoll, P. D. Kucik, B. L. Morales, and L. R. Nunn, 'Invited Review Survey of Value-Focused Thinking: Applications, Research Developments and Areas for Future Research.'. Journal of Multi-Criteria Decision Analysis 20(1/2), 2013, 49 – 60.

Shoviak, M. J. "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, 2001

Vitale, M. R. "The growing risks of information systems success." MIS Quarterly, (1986). 327–334.

Yin, R. K., "Case study research: design and methods". Sage Publications, 3rd edition,2003