Spring 5-14-2015

Decision Support for Holistic IT Risk Feature Selection

Dennis C. Acuña
Dakota State University, dcacuna@bright.net

Decision Support for Holistic IT Risk Feature Selection

Dennis C. Acuña
Dakota State University
dcacuna@dsu.edu

ABSTRACT

The failure or misuse of IT has the potential to negatively impact business objectives. The risk resulting from the failure of IT/IS artifacts can be categorized as IT risk, with holistic IT risk representing the overarching composite of all types of IT/IS failures that can prevent an enterprise from realizing one or more business objectives. The likelihood of holistic IT risk having a significant impact on the global business community is growing, with the Internet of Things capable of spreading IT risk far more widely than the Internet has to date. Feature selection for holistic IT risk can be more difficult than feature selection for non-IT business risk, and can vary from one organization to the next. This research explores the use of decision support and fuzzy logic to design a better method for performing holistic IT risk feature selection.

Keywords

DSR, holistic IT risk, decision support, research-in-progress.

INTRODUCTION

IT Risk

Management of risk to effect good decision making remains a concern if an organization is to successfully achieve its objectives. While identification of risk associated with non-IT business processes is well documented, risk associated with IT is not (Gerber & von Solms, 2005). IT risk is the potential for an unplanned event involving a failure or misuse of IT to threaten a business objective (Westerman & Hunter, 2007). As such, IT risk becomes business risk, and organizations must identify and manage IT risk if an organization is to successfully manage the risk that is inherent in IT decision making. In practice, the IT risk landscape is more complex and subject to more rapid change than the business landscape.

Holistic IT Risk

The notion of IT risk as a holistic measurement is practical (Smith & McKeen, 2009). While an encapsulated view of enterprise business risk can be identified, a similar view of IT risk is not as easily achieved. The feature set that comprises holistic IT risk varies from organization to organization, and can be difficult to identify on a normalized basis with that of traditional business risk (von Solms, 2001). Compounding the need is a rapidly changing IT risk landscape, marked by growing sophistication. Seminal indicators include U.S. Cyber Command, Stuxnet, the Target, Sony, and Anthem data breaches, and realization of the Equation Group. The likelihood of IT risk having a significant impact on the global business community is increasing, with the technology known as the Internet of Things identified by the National Intelligence Council as a disruptive technology capable of spreading IT risk more widely than the Internet has to date (Atzori, Iera, & Morabito, 2010; National Intelligence Council, 2008).

Problem Identification and Motivation

The research objective is the design and development of a better method for performing feature selection for a holistic IT risk feature set. Current practice relies on semantics with minimal use of decision support. New decision support tools incorporating probability and fuzzy logic will reduce the uncertainty and vagueness of semantics, and contribute to effective holistic IT risk feature selection and improved IT decision making.

LITERATURE REVIEW

Holistic Risk Management

Holistic risk management enables enterprise risk management (ERM), the current label for an overall risk management approach to business risk (D'Arcy, 2001). Proper ERM includes all types of organizational risk with the intent of managing risk in aggregate, as opposed to managing risks independently. Holistic IT risk encourages the inclusion of IT risk within ERM from an enterprise perspective, as the analysis of IT risk in a closed environment is unrealistic (Gerber &

von Solms, 2005). Effective analysis of holistic IT risk requires development of new methods to better protect assets vital to the ongoing viability of the enterprise. Achieving an enterprise view of IT risk contributes to a more effective IT strategy (Da Veiga & Eloff, 2007; McFadzean, Ezingeard, & Birchall, 2007; Westerman & Hunter, 2007).

Holistic IT Risk Feature Selection

Holistic IT risk features include IT/IS attributes associated with access, accuracy, agility, availability, change management, confidentiality, cybersecurity, infrastructure, integrity, knowledge management, and project management (Westerman & Hunter, 2007). Features associated with regulatory compliance including Sarbanes-Oxley (SOX), health care privacy (HIPAA), and the payment card industry data security standard (PCI DSS) are also considered. Tacit knowledge is examined as organizations face the dilemma of losing expert knowledge to an aging workforce. Practitioner organizations such as ISACA, ISC2, and PMI provide guidance for attributes associated with specific domains, while government resources such as the NIST SP 800 series contribute cybersecurity features.

THEORETICAL FOUNDATION

The theoretical foundations of this research are grounded in probability theory and fuzzy set theory. The application of probability theory and fuzzy set theory to risk analysis is acceptable, given that both are well suited for dealing with uncertainty. The application of probability theory and fuzzy set theory within decision support is documented within the extant literature (Ngai & Wat, 2005; Rees, Deane, Rakes, & Baker, 2011).

RESEARCH METHODOLOGY

The methodology planned for this research is described in Table 1, and follows the DSR methodology proposed by Peffers, Tuunanen, Rothenberger, and Chatterjee (2007).

Step	Step Description	Step Detail
1	Problem identification and motivation.	Better tools are needed to select the features that comprise holistic IT risk if organizations are to effect better IT decision making to achieve their objectives.
2	Define solution objectives	Design and develop a better decision support method for selecting features that contribute to a holistic IT risk feature set.
3	Design and development	Several IS artifacts will be developed including data gathering tools, datasets, and methods.
4	Demonstration	Effectiveness will be measured using industry practitioners in before-and-after tests, providing a basis for measuring the utility of developed artifacts.
5	Evaluation	Data will be analyzed using sound statistical methods. Focal point will be the measurement of change between current methods and developed artifacts.
6	Communication	Research findings will be submitted for publication. Attention will be focused on the utility produced by the developed artifacts, and rigor of the research methodology.

Table 1. Research Methodology

PRELIMINARY RESEARCH AND RESULTS

There are no findings to report at this time as this paper represents research-in-progress with steps 1 and 2 complete, step 3 in-progress, and steps 4 through 6 not yet begun. Plans include the use of industry practitioners as the sample set from which empirical data will be gathered. Rigor will be emphasized, relevant to the procedures executed in each step. The development platform will be iPython Notebook. Expectations are that this research will improve the process of selecting a holistic IT risk feature set.

Next Steps

Next steps are to complete steps 3 through 6 as described in the research methodology. Completion is scheduled for 3Q2015.

CONCLUSION

Central to this research is the design and development of artifacts that produce utility to enable better IT decision making for selection of features that contribute to a holistic IT risk feature set. Future research opportunities include examination of the findings for development of a machine learning recommender system.

REFERENCES

1. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54*, 2787-2805.

2. D'Arcy, S. P. (2001). Enterprise Risk Management. *Journal of Risk Management of Korea, 12*(1), 207-228.

3. Da Veiga, A., & Eloff, J. H. P. (2007). An information security governance framework. *Information Systems Management, 24*(4), 361-372.

4. Gerber, M., & von Solms, R. (2005). Management of risk in the information age. *Computers & Security, 24*(1), 16-30.

5. Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75-105.

6. March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems, 15*(4), 251-266.

7. McFadzean, E., Ezingeard, J. N., & Birchall, D. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. *Online Information Review, 31*(5), 622-660.

8. National Intelligence Council. (2008). *Disruptive Civil Technologies - Six Technologies with Potential Impacts on US Interests out to 2025*.

9. Ngai, E. W. T., & Wat, F. K. T. (2005). Fuzzy decision support system for risk analysis in e-commerce development. *Decision Support Systems, 40*(2), 235-255.

10. Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for Information Systems Research. *Journal of Management Information Systems, 24*(3), 45-77.

11. Power, D. J. (2013). *Decision Support, Analytics, and Business Intelligence* (2nd ed.). New York: Business Expert Press.

12. Rees, L. P., Deane, J. K., Rakes, T. R., & Baker, W. H. (2011). Decision support for Cybersecurity risk planning. *Decision Support Systems, 51*(3), 493-505.

13. Smith, H. A., & McKeen, J. D. (2009). Developments in Practice XXXIII: A Holistic Approach to Managing IT-based Risk. *Communications of the Association for Information Systems, 25*, 519-530.

14. von Solms, B. (2001). Information Security - A Multidimensional Discipline. *Computers & Security, 20*(6), 504-508.

15. Westerman, G., & Hunter, R. (2007). *IT Risk: Turning Business Threats into Competitive Advantage*. Boston, Massachusetts: Harvard Business School Press.