Oct 28th, 2:00 PM - 3:30 PM

An approach to Information Security for SMEs based on the Resource-Based View theory

Blerton Abazi
University for Business and Technology, blerton.abazi@ubt-uni.net

An approach to Information Security for SMEs based on the Resource-Based View theory

Blerton Abazi

UBT – Higher Education Institution, Prishtina, Kosovo
blerton.abazi@ubt-uni.net

Abstract. The main focus of this proposal is to analyze implementation challenges, benefits and requirements in implementation of Information Systems and managing information security in small and medium size companies in Western Balkans countries. In relation to the study, the proposal will focus in the following questions to investigate: What are the benefits that companies mostly find after the implementation of Information Systems has been implemented, efficiency, how to they manage security of the information's, competitive advantage, return of investments etc. The study should give a clear approach to Information Systems implementation, information security, maintenance, measurable benefits, challenges companies have gone through and a model how to approach Information Systems as a general guide utilizing best practices by the companies that are also supported by the available literature review. A very important place on the research will have also the Information security threats, security management measures and proposed alternatives for organizations to network vulnerabilities from malicious attacks. Since there are several security management frameworks which encompasses also the security management models, my research could be starting with an analyze of the security management, current situation and will end with a proposal for the new approach to information security.

Keywords: Information security, technology, infrastructure, small-medium enterprises, system

Introduction

Small to medium sized enterprises (SMEs) constitute a major part of the global economic activity. Due to the destined characteristics of these enterprises, approaches to information security management that were mainly developed for larger organizations cannot be feasible applied in the context of SMEs. In this research, we intend to present some of the challenges impeding the implementation of information security management in SMEs. We propose a holistic approach based on Soft Systems Methodology to facilitate the development of security management systems within information security problem. We demonstrate the usefulness of our approach through a deep analysis and case study that are currently on the field. The research will be concluded with a brief summary of the findings and presents directions for future work.

As we already know that small and medium enterprise (SME), belong to a special category of organization that requires protection of business information. The risk profile of SMEs in context of information security is becoming equally and more similar to big corporations. Both use technology extensively and would face serious consequences in the event of a data breach. Some factors that affect directly to the low level of security and possibly make hard to build an effective and efficient information security control environment could be, budget restrictions, limited, qualified people on the information security and limited resources.

As security is a common concern among all stakeholders, combating information threats requires collaboration to ensure that the Internet is a secure medium which is needed for building a thriving information society. However, one of the challenges in reaching collaboration is that each group has a different position and approach to how to address security issues and deal with the potential trade-offs related to security and usability. Furthermore, different stakeholders possess different resources that they can invest in countering security threats (Christopher, Meister, ,& Darren B. , 2004). The gap between large and small-to-medium sized enterprises in the information security arena has been increasing substantially as a direct result of the scarcity of resources, available to SMEs.

Our goal in developing a special case on small and medium enterprises (SMEs) and the role of information systems in their competitiveness has been to encourage research into SMEs and highlight the use of new theories and frameworks.

An approach to Information Security related with the Resource-Based View theory

As (Kraaijenbrink&Wijnhoven, F, 2008) mentioned that Resource-based View is considered as one of the most important theories in management, this is also described from the Chandler (1977), (Coase, 1937) and as well Penrose in 1959.

A firm's resources include every asset, processes, information and knowledge which is under the control of the firm and which enables it in order to implement strategies with a goal to improve efficiency and effectiveness (Barney, 1991, p.101)

We would like to tether the information security with the resource based-view theory of firms because, information security investments are considered as a part of general IT investments and therefore the Resource-based View is appropriate for looking up at the information security investments on three dimensions:

• Every IT asset such as data, processes, hardware, firewall and other issues related to the need for protection or resources which provide protection can be modeled as resources

• There are several times when the Resource-based View have been used in the Information Security literature to point the security investment. This was explained clearly by Cavusoglu et. Al (2004) who draw on the RBV to explain hypotheses which are related to organizational sizes, security breached and their link to security investments. Some of the elements of the RBV can be found also in the paper of (Demirhan, 2005)

• According to the numbers, most of the security incidents are caused by the human factor and not from the technical failure, I would like to address the important of the people working on the IT security field and the use of resources.

Investing to the security resources will improve the business processes or it may enable new ones. This is based to the fact that the information security process is intended to protect businesses and their above-mentioned resources because many security process performance have impact on the business process performance, which is a result of the relation business process to security process and is conceptualized as impact. The IT business value generation process, including resources, processes, business and security performances, impacts directly the organizational performance.

Information Systems Strategy approach

The three-stage process has proved to provide a good framework for a thorough analysis of Information Systems Strategy requirements for SMEs based on feedback from users and SMEs.

The main problem for the analysts is the difficulty in separating strategic from operational issues. The nature of SMEs means that the owner is intimately involved with all aspects of the business. The analysts have to unravel the different aspects. It is not uncommon for operational issues to impact upon discussions of business strategy and competitiveness. Models provide some clarity for the analysts. The positivistic or structural models (five forces, value chain) providing clear boundaries can be rejected back easily to the SME to confirm understanding of strategic issues (Blili & Raymond, L., 1993). Standard models such as PESTEL and SWOT are useful to reject back issues and understanding to owners. The strategic opportunities framework is particularly useful. However, the information intensity matrix is of limited value, merely flagging up the importance of information to the SME, but providing few other insights unavailable from other models. Business process modelling proves to be more variable. There is more dependence upon the researchers understanding of the available tools. Generally, SSM is used in a partial manner to understand the problem situation, rich pictures being very informative. The later stages of SSM are used variably depending on the knowledge of the analysts. Value chain analysis is sufficient in many cases to identify systems requirements. In most cases, unlike large corporations, SMEs business processes are directly linked to value-adding activities with few superfluous activities. Thus, the problem becomes one of identifying systems to support existing processes, rather than devising new ones. Additionally, industry sector differences lead to some difficulties with use of tools. This is found particularly in knowledge intensive industries. Resource-based models such as core competences may be more relevant to these organizations strategic grid provides some assistance to analysts in recognizing the limited role of IS in the SMEs and acts as a means of reflecting on the potential use of systems for business growth.

Why integration the IT to SMEs

The rich diversity of different perspectives toward factors that affect IT adoption process is available on a huge body of literature. The review of previous research has identified a number of influencing factors. Most of these perspectives and studies have concentrated on influencing factors such as top management, organizational behavior and characteristics, firms, resources, government, customers, supplier and external IT consultant and vendors (Businge, J. Serebrenik, A., ,& Brand, M. V. D., 2010). Based on a review of the existing literature on IT adoption in SMEs, an integrated framework has been developed and used to classify various issues and factors relative to process of IS/IT adoption within SMEs.

This model merely comprises different aspects of internal and external IT adoption factors (Drivers, influencing factors and barriers) and does not categorize adoption factors based on being drivers or barriers of IT adoption in SMEs. The authors believe that the presented categorization of IT adoption issues and factors through developed conceptual framework can help governments, organizations, managers and IT consultants to achieve clearer understanding of IT adoption process. It also adds further knowledge to the literature while more comprehensive study of IT adoption within SMEs investigating SME-related influencing factors simultaneous with other aspects (drivers, enablers and inhibitors) of IT adoption has been warranted by prior literature. Internal and external factors influencing IT adoption are discussed. This section puts forward a proposed conceptual framework according to the literature and also includes inclusive categorization, as well as review of factors influencing adoption process. Finally, a brief explanation on the IT adoption issues in SMEs would be followed.

Additionally, SMEs are strongly influenced by the standards and culture within their industry sector when it comes to implementing information security. It is dependent on the organization. Some of the SMEs operate based on the knowledge of a few key personnel and therefore the

need for information systems and security management is not vital. However, for some companies which are dealing with more employees sharing the information, then this need to become significantly higher. If an organization is in a competitive industry and one of their products is the key to most or all of their organization revenue, then it is crucial for them to secure that valuable piece of confidential information about their product to ensure competitiveness. Some SME's often implemented information systems and security as they were aware that other companies in the same industry were doing so. Therefore, industry culture is definitely one of the key motivating factors to SMEs

FUTURE WORK TO BE CONSIDERED

According to the literature, there are some lacks on the links between the information security and business sector, and based on this for my research I will address the following questions:

- How the SMEs will build their information security strategy and infrastructure?
- Are the SMEs ready to adopt their intern policies according to the information security standardization?
- How we can divide the security issues between the Information Security and Privacy?

STATE OF THE ART

Based on the literature and papers from experts it is emphasized that information systems and information security has evolved through three waves. Firstly, the technical wave demonstrated by a technical approach to information systems and security. Secondly, the management wave which includes a growing interest and involvement from management to protect information, and thirdly, the institutional wave where best practices and codes of conduct are adopted. Management is focused on proving the information security strength of the organization by implementing information security into the organizational culture, certification, and continuous measurement and monitoring. While viewing information security from a wave's perspective is beneficial, a more valuable approach to viewing information security is from a stages of growth perspective because a stages of growth perspective attempts to identify the antecedents of change over time and provide researchers and practitioners with tools to better study and manage organizational change. (Eurpan Space Agency, 2009) indicated that technology is practical application of knowledge that brings out something entirely new in a completely new way. Technology can be seen as doing new things within an organization. Technology and software development are directly related. This is why software development is important in any technological information system advancement (Terlizzese, 2012). Technology always plays a role whenever an information system is involved in an organization. Infrastructure is best when it is offered as a service. (techtarget.com, 2001) indicated that infrastructure as a service is a provision model where organizations outsource their equipment to be used for support operations including storage, hardware, servers and networking components, while the service is responsible for housing, running and maintaining it. Patel (2006) argued that infrastructural architecture is important especially when adapting to different architectural designs that other companies have embraced within the environment. We have emphasized that adding value is an aspect of quality control that many organizations avoid, yet it contributes to growth in manufacturing industries today. When enterprises adopt value added features like reduction of the risk of occurrence of a safety incident or accident, reduction of the risk of occurrence of an environmental incident or accident, improved assurance of specified product

or service quality, improved actual product or service quality, reduction of product or service delivery cost, reduction of the delivery time for product or service and improved management of resources.

In scientific literature, the need for a proper information security governance methodology led to development of proposals for new frameworks.

References

1. Blili, S., & Raymond, L. (1993). Information technology: threats and opportunities for small and medium-sized enterprises. International Journal of Information Management, 439-448.
2. Businge, J. Serebrenik, A., , & Brand, M. V. D. (2010). An Empirical Study of the Evolution of Eclipse Third-party. In Science and Technology, volume 2009, 63-72.
3. Christopher, Meister, , & Darren B. . (2004). Small Business Growth and Internal Transparency: The Role of Information Systems. MIS Quarterly, 473-506.
4. Coase, R. H. (1937, November). The Nature of the Firm. Economica New Series, Vol. 4.
5. Demirhan, D. (2005). Factors affecting investment in IT: a critical review. Journal of Information Technology Theory and Application (JITTA) 6.
6. Eurpan Space Agency. (2009). www.esa.int. Retrieved from http://www.esa.int/About_Us/Welcome_to_ESA/ESA_Annual_Report_2009
7. Fuller, S., & McLaren, T. (2010). Analyzing Enterprise Systems Delivery Modes for Small and Medium Enterprises. AMCIS 2010 Proceedings.
8. Kraaijenbrink, J., &Wijnhoven, F. (2008). Managing Heterogeneous Knowledge: A Theory of External Knowledge Integration. Knowledge Management Research & Practice.
9. Mehrtens, J. Cragg, P., & Mills, A. (2001). A Model of Internet adoption by SMEs. Information and Management, 165-176.
10. Ormerod, R. (1995). The role of OR in IS strategy development. International Transactions of Operational Research 2, 17-27.
11. Premkumar, G., & Roberts, M. (1999). Adoption of new IT in rural SMEs 27. 467-484.
12. Shewhart. (2001).
13. techtarget.com. (2001).
14. Terlizzese, L. (2012). Trajectory of the Twenty First Century: Essays in Technology.
15. Wynn, M. a. (2006). Delivering business benefits through Knowledge Transfer Partnerships. International Journal of Entrepreneurship and Small Business, 3, 310-320.
16. Wynn, M., Turner, P. , Abur -Robb, O. , & Bruce, A. (2007). Improving Management Control and Business Performance through Knowledge Transfer Partnerships. World Journal of Retail Business Management, Volume 1, Issue 1, 36-44.
17. Wynn, M., & Maldonado, G. (2007). Implementing Enterprise Resource Planning (ERP) Systems through Knowledge Transfer Partnerships: Two Case Studies. International Journal of Management Cases Volume 9 Issue 2, 41-51