International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161

Available at http://inpressco.com/category/ijcet

Research Article

Establishing Effective Guidelines to avoid Failure and Reducing Risk in E-Business

Adel H. Mohammad[Å*], Sameh Ghwanmeh[Å] and Ali Al-Ibrahim[Å]

[Å] Computer Science Department, Faculty of Information Technology, WISE University, Amman, Jordan

Accepted 12 September, 2013, Available online 01 February 2014, **Vol.4, No.1 (February 2014)**

Abstract

E-business is one of the most important business forms. E-business allows organizations to do their business, internally and externally, efficiently and effectively with relatively low costs. Unfortunately, e-business faces several risks which can affect its processes. Additionally, e-business risks are divided into internal and external risks. The paper determines numerous guidelines to deal with the e-business risks. Proposed guidelines represent an effective method to minimize the effect of risk or to avoid it. Presented guidelines are suitable for most types of organizations when used properly and effectively.

Keywords: *E-business risk, Risk management, Guideline to avoid risks*

1. Introduction

There are several definitions to e-business. E-business can be defined as applying information and communication technologies to support all actions of business. Also, e-business can be described as simple, efficient, competent, great revenue, and proficient but it has several risks. Additionally, e-business involved electronic purchasing, buying, processing orders by electronic means, managing customers' service and cooperating with business partners with relatively low costs. Further, e-business is done using internet, intranet, and extranet (http:// en. wikipedia.org/ wiki/Electronic_business).

E-business represents a new era of conducting business. However, the question which must be answered here is whether e-business is fully trusted and secure or not. Actually e-business has serious risks everywhere and every time, so managers have a heavy duty to identify risks and minimize their effects. Basically, types of risks come into different forms, and they may come from inside the organization or outside the organization. No doubt that all types of business face certain types and degree of risks. E-business also faces different forms of risk. Managers must know that the first step in managing risk is started from identifying risks' sources. Beside that we have to know that risks vary between companies based on their types and sizes (Patrick D. Gallagher et al, 2012).

In this paper common types of risk have been investigated, which may affect e-business to be used later in building our guidelines to minimize or avoid the effect of risks and failure in e-business organizations. Furthermore, the paper determines numerous guidelines to deal with the e-business risks.

*Corresponding author: **Adel H. Mohammad**

2. Risk Management and Risk Sources

Risk can be defined by demonstrating to anything that may present threat or may limit the capability of e-business. Also it can be unexpected or expected event that is danger or can limit organization capability. Some forms of risk are physical, such as destruction of a building, fires, and theft which are outside the scope of this paper. This paper focuses on assessing the risk on e-business and how to avoid it (Patrick D. Gallagher et al, 2012, https://en.wikipedia.org/wiki/Risk_management). Risk management is an important issue as it provides the vision to deal with risks. Risk management has different definitions. It can be defined as the identification, evaluation, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or the impact of unfortunate events. Also, it can be defined as the process of identifying risk and all of its resources, and then taking all necessary steps to minimize its effects to a minimum level. Further, risk management could be defined as the process of scientifically thinking about all sources and opportunities of risks (Arnold Johnson et al 2011; Gary Stoneburner et al 2002; Gary Locke et al (2010), Fana, M. et al 2007).

Risk management answers several questions, such as what may be go wrong and how we can prevent it and finally what we must be done if risk occurs. Risk management plays an important function in defensive the organization and its capability in accomplishment its job. In e-business area, risk management is very important issue and actually it is a part of IT security program. The field of information and communication technology (ICT) is responsible for protecting e-business and managing all suitable involved technology accurately (Arnold Johnson et al, 2011; Gary Stoneburner et al, 2002, Gary Locke et al, 2010). Currently, organizations face several types of risks such as program management risk, investment risk, budget risk and security risk. Performing effect risk management requires operation in a complex and connected environments. Providing the suitable and necessary response for each type of risk is a key success factor. Additionally, the main core of risk management is to minimize the influence of risk. In addition, risk management deals with rational evaluation of actual level of risks (Gary Locke et al, 2010, Fana, M. et al, 2000).

The process of risk management requires IT managers to balance between operational costs of protection their organization and the accomplishments by protecting their IT system and data (Culp, Christopher , 2001). The main objective of risk management process is to classify all types of risk, to deliver a suitable methodology to minimize the probability of risk occurrences and to minimize its affect in case of existences. It is necessary to recognize that the objective of risk management is not risk avoidance. However, in risk management we are looking onward to minimize its probability of occurrences and in case of occurrence we aim to minimize its affect (Culp, Christopher, 2001; Shahram Gilaninia, 2013; https://en.wikipedia.org/wiki/Risk_management).

Actually, managing risks involve several strategies. These strategies include transferring risk to another party; minimize the impact of negative results on organization, and accept the impact of risks (Eduardo Rodriguez et al, 2010; Patrick D. Gallagher et al, 2011).

Risk management is a complete process that requires organization to conduct the following (Gary Locke et al, 2010; Fana, M et al, 2007; Culp Christopher et al, 2001; Gagandeep Singh et al, 2012 ; http://en.wikipedia.org/wiki/Business_risks):

a) Frame risk, in this phase organization creates the risk context.
b) Assess risk; the goal of this phase is to identify threats to the organization and internal or external vulnerability.
c) Response to risk when it is identified; the aim of this stage is to provide a consistent response to risk.
d) Monitor risk; the target of this stage is to verify that planned risk response measures and information security requirements are satisfied

The internal risk may result from several factors; some of them are internal while others are external. The internal factors are appeared from the inside of organization and they can be approximately controlled. Examples on these factors are human factors, management, physical failures of some equipment, and operational factors such as advertisements. External risks are appeared from outside the organization but they cannot be controlled as the internal factors; global economy factors such as market, natural factors such as earthquakes, and political factors such as low and legislations are good example on external risks. Nevertheless the types of risks, risks are mainly related to competitor, employees, customers, technologies, environment, laws, regulations, and operations (http://en.wikipedia.org/wiki/Business_risks). Technology used and emergent technology is a critical factor that can cause huge risks. In the information age and digital era some technology died before they even born. Therefore, large organizations have to use appropriate knowledge management system (KMS) to minimize the effect of potential risk (Eduardo Rodriguez et al, 2010).

Before introducing literature review, main sources of risks are discussed. Based on previous related studies, risk sources can be divided into two types. Several studies categories risks into two main types based on its source such as internal risks and external risks. Following, we will discuss this type of risks which come from both inside and outside the organizations [Fig. 1] (Jensen et al, 2006; Jan Boone et al, 2000).

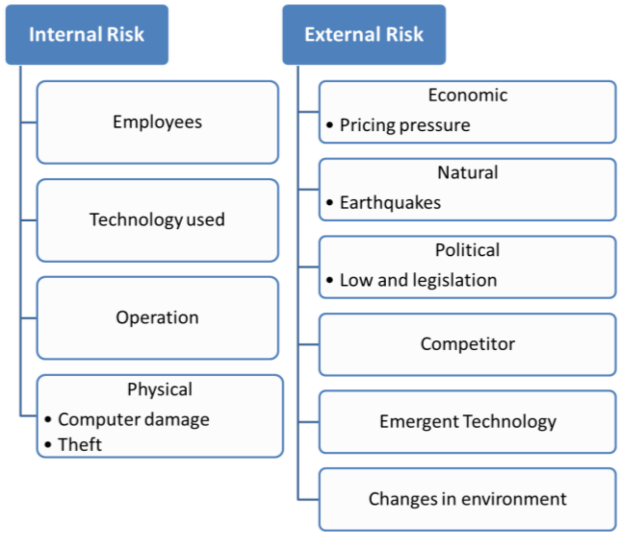

Figure 1: Internal and External risk sources.

3. Literature Review

Michael Ettredge, M. and Richardson. V. identify the risks to e-commerce using a dissimilar sample of internet and other firms. They suggest that managers of firms disclosing controllable e-risks potentially can reduce their costs of equity if they ameliorate the controllable risks (Michael Ettredge et al, 2002).

Dominik D. Lambrigger proposes a new approach. The approach allows a combination of internal data, relevant external data, and expert opinion to estimate the parameters of the risk frequency and severity distributions. Additionally, the approach is simple and suitable for operational risk quantification (Dominik D. Lambriggeret et al, 2007).

Nastase, F. shows that information and communications technology (ICT) and IT security are mainly responsible for making sure that technology risks are managed properly. Also, it can be seen that these risks originate from the setting and using of IT assets. Furthermore, author shows that the tools of risk management provide advantages to an organization by improving understanding of operational environment (Floarea Nastase et al, 2007).

Miller, H. and Engemann, K. discusses types of risks presented in e-commerce. Also, the authors discuss e-commerce risks and risks in other business environments. Authors show that e-commerce risks are similar to risks encountered in other business types. Further, authors categorize three risks in three primary areas: information risks, technology risks, and business risks (Miller, H et al, 1996).

Nathwani, J. and Narveson, J. provides three principles and general framework of reasoning for managing risk in public interest. Principle 1 "Risks shall be managed to maximize the total expected net benefit to society" Principle 2" The safety benefit to be promoted is life-expectancy" Principle 3" Decisions for the public in regard to health and safety must be open and apply across the complete range of hazards to life and health (Jatin Nathwani et al, 1995).

4. Guidelines for Risk Management and Avoidance in E-Business

This section shows how to setup major guidelines for dealing with risks to minimize their possibility of occurrence and to deal with them when they occur. These guidelines proposed based on extensive reading and assessment of literature review. Managing risk is not an easy process; it is a multiple side accomplishment that requires the participation of all members of organization. We have demonstrated several types of risks, but not all e-business organizations really face all types of risks. The type, size, and location of organization play a main role for determining the kind of risk it may face. Figure 2 demonstrates internal risk guidelines.

Every employee has a great knowledge in his mind which may be lost from the company when he leaves his work or he moves this knowledge to another competitor companies. So it is very important issue to never leave so many important knowledge hold by only one staff member. This is done by applying a proper knowledge sharing methodology which means applying appropriate activity and process to interchange knowledge properly between employees. Organization applied proper knowledge sharing system between employees would minimize the risk of losing any employee. Technology used is a critical aspect in success or failure in any organization. Using appropriate knowledge management system (KMS) is the key factor for success and it minimizes the effects of technology risks. Internet and information technology have a significant effect on e-business. Rapid development and high demand on technology increase the risks and their effect of e-business. Solving this problem requires professional managers to identify correctly suitable KMS.

Operational risk management (ORM) can play a significant role in risk management. ORM includes assessing and implementing risk. Results of ORM are acceptance, mitigation, or avoidance of risk. The idea of ORM is to help managers, leaders, and decision makers, to consider risk management as a routine of their plans. Relating to physical risk there are two views. The first one deals with physical equipments which are inside organizations. In this issue organizations have not to use plug and play technology. The second view which is outside the aim of this paper deals with securing the building from outsiders and securing departments from insiders. The solution is not only using cameras inside departments but also at the borders of the organization. Further, using secure cards to allow only the employees to enter their departments.

Figure 2: Internal guidelines to avoid/minimize risks.

The following demonstrate details of external risk sources and how it can affect organization and how organizations have to deal with these sources of risks to minimize probability of occurrence and how to deal with it in case of occurrence. Figure 3 demonstrates external risk guidelines. Starting with economic factors, no doubt that organization priority is altered based on economic change. These changes in priorities are important if organization want to survive. One of the main goals of risk management is to keep business running smoothly and accurately in case of environment and economic changes. Here, establishing suitable standards is very important and it is the obligation of decision makers. Alteration in economy involves a change in expectation of organization customers, vendors, partnership. In summary, organizations have to expand their planning process to take into consideration the potential effects of change.

Some types of natural risks are hard to deal with such as disaster or flooding. But some natural risks can be predictable and managed especially in the e-business world. Forces of nature can cause enormous amount of risks to any organization regardless of its type. Actually if the business is fully digitized and has no physical locations it will be affected less than traditional business with physical location. Frequent and planned backup of data in distributed and several locations can minimize the effect of natural risks. Analyzing the effect of political law and regulations is significant. Political risks management started at a high level management. Top level manager must understand local and global regulations inside the country which they want to capitalize inside. Also understanding regulations of local regulations can directly affect performance. Finally international and global company must follow a systematic methodology to deal with political issues.

Understanding competitor organization and their expertise is the first point in dealing with competitor risks. Organization managers have to plan early how to deal with competitors. Monitoring competitor advanced can help avoiding any unexpected event. Monitoring competitor price, new products, and expanding business is a key success factor. Also, understanding the innovations of competitors permits organization and mangers to identify their position in market and to take appropriate decision. It can be seen that new technology carries many enhancements to organization. But rapid deployment of new emergent technologies creates risks in many cases. Spending millions of dollars for acquiring a specific type of technology and then the existence of another technology with lower costs could be consider as a disaster. A technology risk advisor inside an organization requires helping decision makers in their organizations about emerging technology. Lack of knowledge and experience about new emergent technology is critical and may increase the effect of lost or damage in organizations. It is important that the risk advisors to keep an eye on new emergent technology, industry, market and user needs.

Finally, global financial crisis have a great effect in all countries and all business. Certainly, e-business is one of the areas which affected by global crisis. World economy faces several significant challenges; these challenges produce several signals of unease in financial markets. Therefore, all organizations have to reassess their models in risk management. In addition, organizations have to advance their process regarding risk and global environment.

Figure 3: External guidelines to avoid/minimize risks.

5. Conclusion

The paper has dealt with three main areas which are important for any company to do its work efficiently. It demonstrates risk, risk management and risk sources. The internal and external risks are presented in a clear manner and the most types of risks are demonstrated in a simple figure (Fig. 1). The main core of this research is depicted in Fig. 2 and Fig. 3. Internal risks are represented by employees, technology used, operation and physical factor. It can be seen that internal risks can be avoided or minimized by the guidelines proposed in section 4. This can be accomplished by applying knowledge sharing, using appropriate KMS, and managing risks as a part of planning in earlier phases of development and applying physical security at multiple levels. Related to external risk guidelines, several guidelines have been provided. External risks can be avoided or minimized by the guidelines proposed in section 4, including: applying proper planning, suitable and planned backup, systematic global methodology, knowing your competitor capability and future trend, keeping an open eye on markets and competitors, and finally reassessing business models to face risks.

Acknowledgments

The authors are grateful to WISE University, Amman-Jordan, for the financial support granted to cover the publication of this research article.

References

http://en.wikipedia.org/wiki/Electronic_business.

Patrick D. Gallagher, Rebecca M. Blank (Sept 2012), U.S. Department of Commerce, *National Institute of Standards and Technology*, Under Secretary for Standards and Technology and Director, Guide for Conducting Risk Assessments.

https://en.wikipedia.org/wiki/Risk_management.

Arnold Johnson , Kelley Dempsey , Ron Ross , Sarbari Gupta , Dennis Bailey (Aug 2011), Guide for Security-Focused Configuration Management of Information Systems , *ACM National Institute of Standards & Technology*.

Gary Stoneburner, Alice Goguen, and Alexis Feringa (July 2002), Risk Management Guide for Information Technology Systems, *National Institute of Standards & Technology*.

Gary Locke, , Patrick D. Gallagher (Feb 2010), Guide for Applying the Risk Management Framework to Federal Information Systems, U.S. Department of Commerce, *National Institute of Standards and Technology*.

Fana, M. NengPai Linb, Chwen Sheu, (2007), Choosing a project risk handling strategy: AnAnalytical model. , *International journal Production Economics*, 112, 700-713

Culp, Christopher L.,(2001). The Risk Management Process, *John Wiley & Sons*, P.10.

Shahram Gilaninia, Hossein Ganjinia, Batool Asadi Mahdikhanmahaleh,(2013) difference between internal and external supply Chain risks on its performance**,** *singaporean journal of business economics, and management studies* Vol.1, no.8

Eduardo Rodriguez, John Edwards, People, Technology (2010), Processes and Risk Knowledge Sharing, *Electronic Journal of Knowledge Management*, Volume 8 Issue 1 (pp139 - 150), available online at www.ejkm com.

Patrick D. Gallagher , Gary Locke (March 2011), Managing Information Security Risk Organization, Mission, and Information System View, *National Institute of Standards and Technology*.

Gagandeep Singh (2012), Use of Knowledge Management techniques for Risk Management, Master's Thesis, Department of Civil and Environmental Engineering, Chalmers University of technology.

http://en.wikipedia.org/wiki/Business_risks.

Jensen, Berit Aadal, (Jan 2006) Technological Risks - Emerging Technologies and Co-existing Risk Conceptions Thesis, http://rudar.ruc.dk/handle/1800/2077.

Jan Boone, (2000), Competitive pressure: the effects on investments in product and process Innovation, *RAND Journal of Economics* Vol. 31, No. 3, Autumn, pp. 549–569.

Michael Ettredge, Vernon J. Richardson ,Proceedings of the 35th *Hawaii International Conference on System Sciences* – 2002, 0-7695-1435-9/02.

Dominik D. Lambrigger (2007), The quantification of operational risk using internal data, relevant external data and expert opinion, *Journal of Operational Risk* ,(3–27) Volume 2/Number 3

Floarea Nastase (2007), Risk Management for e-Business **,** *Revista Informatica Economică*, nr. 3 (43

Miller, Holmes E. and Engemann, Kurt J. (1996); A methodology for managing information-based risk; Information Resources Management Journal; 9:2; 17-24

Jatin Nathwani (June 1995), Jan Narveson, 3 principles for managing risk in the public interest, *Risk Analysis*, Rev 1.