The process of Risk management for E-business

Erion Lekaj
European University of Tirana, Albania

Donika Kercini
European University of Tirana, Albania

Abstract

In the new Internet economy, risk management plays a critical role to protect the organization and its ability to perform their business mission, not just its IT assets. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. The risk management is an important component of a IT security program. Information and communications technology management and IT security are responsible for ensuring that technology risks are managed appropriately. These risks originate from the deployment and use of IT assets in various ways, such as configuring systems incorrectly or gaining access to restricted software.

Keywords: risk, e-business, threat, vulnerability.

Introduction

E-business continues to radically alter the competitive landscape in most industries. And the equipment leasing industry is no exception. Innovative Web sites now bring information and services to the end customers that were once only available through intermediaries and at high costs. They can now trade securities, complete banking transactions, access suppliers, process invoices, apply for loans—and yes complete leasing transactions—all on-line, quickly and inexpensively. E-business is dramatically reducing the cost of critical business processes as well. Large financial services companies and institutions are slashing various expenses through the use of Web-based exchange systems that allow the end user, the employee, to instantly identify and transact for needed products without legions of internal support personnel or external intermediaries. Yet, despite these marketing and operational opportunities, e-business brings with it risks never before encountered by financial services organizations. Access through the Internet brings heightened concerns about security, information protection, and privacy. The rapid growth of an Internet customer base and the need to constantly update Web sites, brings technology issues regarding scalability, manageability and business continuity. These issues have also led to changes in regulatory requirements that now must be addressed faster than before. The main purpose of the study was to provide a basic overview of the kinds of e-business risks companies have faced and the techniques used to manage these risks using a questionnaire

The questionnaire was broken down into three main sections. The first section included a table that gave the responding managers a free hand to identify key problems or

risks that arose and the techniques used to manage these risks. The objective here was to understand which types of risks were the greatest concerns for management, whether risk management was in general a priority, and what techniques were most commonly used to mitigate specific risks.

The second section requested the respondents to place the aforementioned risks into a given list of categories and indicate any outliers. This section was testing out the validity of the Seven Risk Categories Framework.

The third and final section examined the types and activities of the respondent organisations. This would help in determining whether there could be a relationship between the type of e-businesses and the prevalence of specific risks. Further research on a larger sample size would be required to validate this kind of relationship with any certainty.

E-Business Risk Categories: When asked to identify the difficulties that occurred in achieving the e-business goals, 34% of the problems cited were classified as risks associated with the commercial environment, 21% were related to the strategy, 23% were linked to technology. The rest were mainly distributed among the other areas of the of the Seven Risk Categories Framework

There was only one mention of a problem that fell outside of the seven categories, and this was a special case pertaining to an atypical relationship between the e-business and its main investor. Therefore, the Framework seems to encompass all key risk types.

Each problem or risk mentioned was usually classified in more than one of the seven risk categories. For example, problems perceived as personnel risks (defined as personnel attitudes to data security, defamatory e-mails, inaccurate advertising on the web) were also frequently identified as technology and business process risks.

Problems classified in all other categories of risks were generally linked to the commercial environment too. These overlaps suggest some connection between categories; however, further research will be required to explore the exact nature of the relationships.

Risk Management Techniques: The problems mentioned may fit into the Seven Risk Categories Framework, but what exactly were these issues and what techniques were used to manage them?

This section details those problems and outlines the risk management approaches of the respondent organisations.

Commercial Environment Risk Category: Almost all of the respondents mentioned an issue that fell under the Commercial Environment Risk Category. Regardless of the type of e-business—whether a start-up, spin-off, incumbent, B2B or B2C—the greatest problem in this area was the reluctance of their target audience to use the Internet service.

To manage this risk, the respondents used methods such as promotional programmes, offline support, and aggressive public relations (PR) to advertise early wins. Education on security and general online benefits was also viewed as important.

E-businesses that were established within a large corporation leveraged the brand value and distribution channels of the parent companies to drive enrolment and usage. This, however, often raises the issue of reputation risk. Could the e-business

somehow harm the goodwill of the entire organisation? The discussion on Strategy Risk Category explains more.

Other concerns of the commercial environment included increased competition and the negative market sentiment towards the New Economy. To beat the competition, companies identified unmet wants/needs through extensive market research and altered product/service offering. To mitigate the downturn in market sentiment and valuations, managers moved swiftly to implement plans, demonstrate progress, and firmly establish the e-businesses; thus, preventing the abandonment of worthwhile projects.

Strategy Risk Category: Risks associated with the strategy of the business were the second most commonly mentioned. The respondents referred to a diverse range of issues, but the main issue that encompassed overall concern in this category was the problem of an unproven business model.

Lack of benchmarks to forecast returns, unpredictable growth of newly defined markets, and challenges in providing simple interactions for all target segments made it difficult to assess the sustainability, acceptability and viability of the e-business.

-experimentation after extensive research and detailed market analysis,
-diversification of spends to spread risk,
-allocation of spends purely contingent on performance,
-continual development of innovative revenue generating options, and
-continual improvements on products/services to cater to target needs.

Corporations with existing offline businesses were more concerned with whether the new venture would be acceptable and viable under the umbrella of the parent company. More specifically, many were concerned with whether and how the e-business would modify the company's image and reputation. To avoid any negative effects, careful management of customer expectations, phased rollout of service, and content testing were some of the risk management techniques used.

Technology Risk Category: Two-thirds of the respondents identified technology-related risks as problems in achieving their e-business objectives. These risks are summarised in Table 3.

Integration with existing internal and external systems was a major concern for many. Incompatibilities between systems are often significant hurdles for companies that work in an environment in which information is offered and/or required in real time. To control this potential problem, companies used interfacing programmes, strong development teams and good project management. Clear definition of milestones was critical.

Other technology risks included hardware failure, slow down in running applications, and damage to the integrity of the company systems.

Business Process Risk Category: The problems indicated here are generally those that hinder the organisation's ability to deliver the right goods and services, as shown in Table 4.

To deliver the proper quality and at the right speed, respondents have developed shared portals, increased resources, redefined functions and priorities, and upgraded offline distribution channels.

Escalating cost of delivery has led to tight budget controls and has driven companies to

understand optimum workflow in order to create templates and automate processes.
Criminal Activity Risk Category: In e-business, the potential impact of criminal activity can be reduced by creating an appropriate technical architecture and surrounding processes that provide identification and authentication, authorisation, non-repudiation, privacy, and accountability.
Secure identification systems with a combination of password and physical card, firewalls, notification on responsibilities, and encryption of critical information were some of the techniques mentioned to provide maximum protection and safeguards. Contingency and incident response planning were also suggested.
The respondents in the financial services sector expressed the greatest concern with security. This is perhaps due to the value of online financial information that hackers find tempting to access. With illegal acquisition of the information, hackers could manipulate data to alter account balances, misappropriate funds, completely shut down the website, and even cyber-extort the bank with an offer to sell the stolen information back.
Legal Systems/Regulations Risk Category: Law, rules, and regulations can be a challenge for e-businesses to follow. With legal and regulatory requirements in a constant state of flux, the outcome is considerable ambiguity with respect to contracts, signatures and commitments. The difficulty is further compounded by the different requirements for different markets.
In order to avoid problems in this area, companies have kept abreast of the latest e-business legislation, implemented content monitoring procedures for compliance, and developed processes to ensure alignment with risk management groups across markets.
Personnel Risk Category: The questionnaire gave the following examples of personnel risks: personnel attitudes to data security, defamatory e-mails, and inaccurate advertising on the web. Respondents usually mentioned these alongside technology and business process risks. As such, these issues have already been discussed in the sections above.
The respondents to the survey gave examples of other people risks including the evolution of employee roles and responsibilities that create insecurity and displacement of staff members, lack of available skills, and limited managerial-level support. Table 5 outlines some of the approaches used in managing these problems.
Risk Management Practice: To gauge the level of risk management in the e-businesses, we asked the respondents to indicate whether the problems mentioned were identified (in advance) as possible risks and if so, what types of preventive measures were taken to manage these risks. Additionally, we asked whether risk management, in general, was considered at the time when the e-business operation was first planned.
The results reveal that 72% of those problems mentioned had been foreseen as risks. But only 56% of the respondents had considered risk management during the planning phase of the operation. These numbers suggest that, in many cases, risks were evaluated at a later stage--perhaps during the development phase of the e-business.
For those 12% of the respondents that indicated <u>some</u> progress in risk management during the planning phase, they pointed out that most technical scenarios were considered, but little planning was made on the commercial side.

The 32% of the e-businesses that did not assess risk from the beginning felt that too much risk analysis created obstacles and impeded first-mover advantage.
These statements suggest similarities between the management of e-business risks and traditional business risks. Further research will be conducted to verify this assumption and identify the actual area(s) of similarity.

Conclusions

The main objective of the questionnaire survey was to provide a basic overview of the types of e-business risks companies have faced and the techniques used to manage these risks.
The data collected from the 36 respondents has confirmed that the Seven Risk Categories Framework is valid. The survey results also established that risks associated with the commercial environment, strategy and technology have been the most common concerns for companies today.
In the respondent organisations, risk management was generally considered, but not always in the planning phase of the e-business operation. Some evaluated risks as the e-business developed and only looked at technology-related risks from the beginning, and others viewed too much risk analysis as an obstacle to product/service speed-to-market.
From these preliminary findings, the following topic areas have been highlighted for further investigation:
-the relationship between risk categories,
-the identification of similarities and differences between traditional risks and e-business risks, --- and the relevance of risk management models.
Case study interviews will be conducted to obtain a more in-depth understanding of risk management practices and general perceptions on e-business risks.

References

Buecker, J. D. (2006). Enterprise Security Architecture, IBM Redbooks.
Hamel G. and J. Sampler, (1998). The e-Corporation: More than just Web-based, It's Building a New Industrial Order, Fortune.
Mason S. (2000). Electronic Signatures: The Technical and Legal Ramifications, Computers and Law, volume 10, issue 5.
Nastase, P. Nastase, Fl. (2006). Security Controls to Protect Information Systems, Proceedings of the 3rd International Conference - Economy and Transformation Management, Editura Universității de Vest, TimiŞoara.
Nastase, P. Nastase, Fl. R. Sova (2007). IT Audit Trends within Framework of Balkan Countries, The Balkan Countries' 1st International Conference on Accounting and Auditing (BCAA), Edirne- Turkey.
Voss C. (2000). Developing an eService Strategy, Business Strategy Review, volume 11, issue 1, Spring.
http://www.isaca.org
http://www.enisa.europ