International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-5, March 2020

Assessment of Risks in Information Technology Projects

Malaya Nayak

Abstract: ***The risk associated with information technology is quite big especially when it comes to using, own, operate, and select information technology systems for an organization. The risk associated with information technology is possibly termed as a business risk. It includes IT-related prospects that may affect businesses. This can be achieved with both a questionable relapse and scale which threatens the alignment of key objectives and goals. The study is based both on empirical studies and on true case analysis. The study found that top management understands the essential part of technology development in organizations that are infamous for corporate viability and efficiency because of the use of IT hardware and computer software.***

Keywords: IT project, organizational risk, risk management, risk assessment, software development.

I. INTRODUCTION

The risk may be the usual term for Information Technology / IT Systems (IT / IS) accounting into each sector. IT applies to specialized equipment and organized techniques basically focused on production, supply-orientation and creativity, and concentration distribution. In contrast, IS, in general, and especially, is a commercial application, that is based on IT. Although various interpretations advertised, from diverse viewpoints, the risks to the IT and its development projects in this medium is characterized as the susceptibility to such dubious predictive occasions as a foreseeable setback and damage. This research article classifies IT risks in 3 types:

(1) Technological as well as operational prospects;
(2) Data and security risk; and
(3) The organization, prolongation and human threats.

It is impossible to believe that all vital information could be properly protected from any assault exquisitely (Decker, 2001). An intended intruder will destroy everything with infinite confidence and properties. Instead of removing any threats, a feasible solution would be to make security safeguards deliberately to ease or reduce risks to decent limits (Peltier, 2005). IT infrastructure for project development follows certain regulations/protocols for the minimization of threats. In IT procedures credibility ensures unlicensed modification and cover-up of data. Access is about the secure connection to data transfer by approved users, in particular in terms of assaults including conflict with IT data systems.

II. IT RISK MANAGEMENT

Risk management may be divided into three processes as shown in Figure 1

Revised Manuscript Received on March 30, 2020.
* Correspondence Author
Malaya K Nayak*, U-Com Software Private Ltd.

Liability is the obligation of all the parties concerned with commitments and the traceability of the actions. Data protection is often said to be simply a matter of luck control (Schneier, 2000). (NIST, 2002; Farahmand, Navathe, Sharp, and Enslow, 2003; Alberts and Dorofee, 2002; Vorster and Labuschagne, 2005).

This ought to be noted that these types are not commonly used, although, most people share basic ingredients for risk assessment and threat reliefs (Microsoft, 2004; Hoo, 2000). It is also a common understanding. Opportunities for evaluating and processing profitable information, frames of security flaws, plausible risks, probable consequences of such threats as well as the risks posed by the framework are mostly observed.

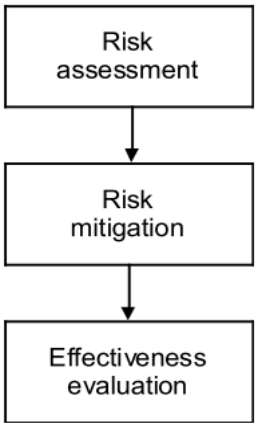

Fig 1.Risk management steps

Risk management would essentially be a collegiate study without any of the risk reduction procedures. Moderating threats can be a guide to prioritizing the risks that have been established well into the risk analysis through implementing action to reduce the higher priority risks under the conditions of the finite assets of a company in particular. The aim is to determine and confirm that the goals for the moderation of risks have been achieved. If not, it may be necessary to upgrade the necessary actions for risk evaluation as well as restraint. Essentially, the determination of feasibility offers feedback to the 2 main sources to ensure accuracy. However, the setting is often dynamical for a company. A continuous review should be carried out to improve the strategy of risk management of new/unused details.

III. IT RISK ASSESSMENT

It is incomprehensible to realize which attacks will take place for a certain process. What else might result depends on the uncertainties/threats. Instead, the probability relies upon the occurrence of a risk. Too, the danger isn't much of a risk if the secured structure is not defenseless to the threat or if the possible loss is not significant.

Furthermore, the threat is a risk function as well as the predicted impact of risks. The risk assessment comprises several phases to evaluate capital, flaws in the system, potential risks, risks evaluation including expected influences.

A framework of the procedure is revealed in Figure 2.

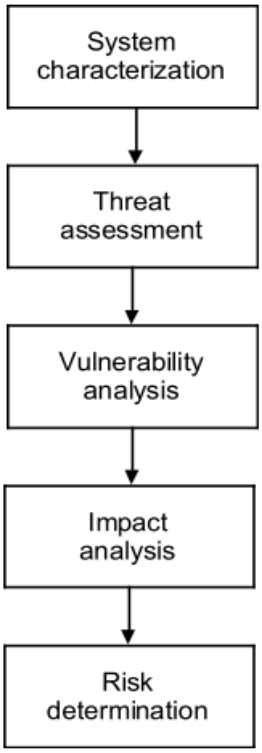

Fig 2. Steps in risk assessment

1. *System characterization*: It is clearly necessary for the data to be understood in order to secure, importance and dependencies of the structure which underpin the capability, controlling and transfer of data (equipment, computer program, processes, formats, humans, etc.). The technology engineering (IT) paradigm is sometimes referred to periodically. A number of faculty interviews, surveys, information surveys, on-site evaluations, and computerized checking can make Framework Interpretation possible. Some of them, like the Cheops, iNetTools, strobe, SamSpade, NetScanTools, Winscan, Nmap, netcat and CyberKite are available in the category of paid and open-source applications.

2. *Threat assessment*: It is not possible to prepare a defensive strategy without recognizing what it should defend against (Decker, 2001). There is a possibility that the IT staff may experience any accidents or discomfort. The possible factors or origin of risks are worth identifying. While damaging assaults from human source information could first take center stage, the sources of threat are often not primarily human. It is difficult to classify malicious human perpetrators because their inspirations and behaviors may vary widely (McClure, Scambray and Kurtz, 2001). Human perpetrators could be explicitly labeled as internal or external.

The standard internal intruder may be a dishonest agent who tries to strengthen the company or an untrustworthy contractor for exclusive data or personal data that is accessible to other workers. External threats in some cases are the main trouble as they undoubtedly have access to the important resources of an enterprise and perhaps have high-profile network profiles (e.g., Unix root or Windows administration). In contrast, foreign attackers have to pierce the resistances of an enterprise (such as firewalls) in order to catch them and then it would be difficult to pick up root or management benefits.

3. *Vulnerability analysis*: In the sense of risk, threats should be recognized. An impairment or exposure could also be victimized as an insufficiency. Perhaps the easiest mode to distinguish between exceptional flaws. Software and device administrators send error alerts and flaws almost never with certain products in accordance with updates. Several scanners for paid and open source applications for determining insecurities like SARA, Satan, Nessus as well as Saint, are usable. Basically, these scanners have a repository of security flaws and test a framework for all these faults.

4. *Impact analysis*: The effects on the company of each risk relies upon several uncertain variables: the chance that the risk occurs; malaise from the successful event; as well as the recurrence of the risk repeats. In hone, these factors can be difficult to evaluate, so various ways of calculating and integrating them in an inquiry into the effect are available. The analysis of risk impacts can range from completely quantitative (numerical) to subjective (graphical) or other. It is ideal to calculate the exact possibility of each risk, but a good estimate is more realistic and reliable. The possibility relies on the danger aspect.

The analysis of subjective results can aim to categorize impacts into broad categories like strong influences, low influences, and moderate influences. In comparison, predictive modeling aims to relate investment to an appropriate danger potential, defined as a simple prediction of failure. If the risk recurrence (e.g., depending on reliable information) is to be determined, the subject of SLE and re-occurrence is the so-called annualized loss expectancy (ALE). (Blakley, McDermott, and Geer, 2002; NBS, 1975):

$$ALE = SLEx\ (annualrateofoccurrence)$$

5. *Risk determination*: For each threat, its likelihood can be multiplied by its impact to
determine its risk level:

$$Risk = likelihoodximpact$$

High probability and a great deal of impact are the major genuine risks. A very low-probability higher risk of effect might not even be commendable, and a small-probability danger of minimal influence can also be viewed as being less real. Each danger can be divided up into multiple risk levels depending on the possibility and effect object. When planning the risk relief, high risks should be taking and perhaps most important into consideration. Marginal threats should also be moderated but perhaps less vulnerable. Finally, low risks could be dignified without relief or moderated if enough resources exist.

IV. RISK MITIGATION

It can be acknowledged reliably that every organization has restricted security assets. There is no way to protect ourselves from every possible threat. A certain degree of chance can be worthwhile in expansion.

The approach of risk reduction is to devote minimal assets deliberately to change insufficient hazards into dignified ones. Risk reduction can be a mixture of specialist and non-specialized modifications. Specialized improvements involve security devices (e.g. audits, authentication, firewalls, place interference systems, data security, application anti-virus software, tracks, refurbishments) as well as the maintenance of this infrastructure. Non-technical changes may involve changes in methodology, customer preparation as well as safety attention.

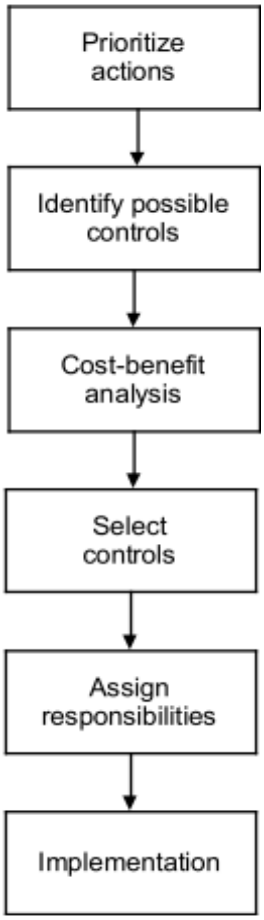

Fig 3.Risk mitigation steps

1. *Prioritize actions*: The risks with their comparative levels distinguished by a chance assessment will suggest what should be done. Obviously, the risks at unsatisfactorily high levels should be addressed most certainly. This move should draw a positioned list of requirements to resolve the recognized dangers.

2. *Identify possible controls*: This move explores all possible risk reduction operations. Many controls seem to be more practical or practicable than many other regulations, but afterward, the certainty is remedied. The outcome could have been a collection of management options to promote analysis.

3. *Cost-benefit analysis*: The emphasis of risk management is the analysis of cost/benefit trade-offs in each regulation approach (Gordon and Loeb, 2002; Mercuri, 2003). This move accepts that the capabilities of a company are limited and should be considered viable in growing risks. In the incident that it can be recovered by the decrease of risk, control is as advantageous literally and figuratively. Costs might also be involved with the preparation of workforces, time, additional human resources and implementation of arrangements. Too much power may affect the IT framework's competence. Cases are helpful to validate system-level tests on clients and servers but can that the implementation of systems. This might be an additional cost, yet difficult to assess.

4. *Select controls for implementation*: The cost-benefit analysis from the previous stage is used to determine the policies to be revised in order to achieve the goals of the enterprise. The new regulations would obviously need a budget and the budget has to be tailored to satisfy the other policy criteria of the organization. Therefore, the ultimate decision of tests to carry out does not rely so to speak on the need for the operation but also on the organization's conflicting needs. Companies spend 0,05% of their earnings on basic protection, as was reported (Geer, Hoo, and Jaquith, 2003).

5. *Assign responsibilities*: Finally, success relies on workers with appropriate skills. The team staff can be accessed within an organization; however, an organization may elect to nominate a third party for a number of different reasons.

6. *Implementation*: In the final step, the selected controls must be implemented by the responsible personnel.

V. RESULT

The analysis of subjective results produced effective outputs into broad categories like strong influences, low influences, and moderate influences. In comparison, predictive modeling generated a fesiable output of an appropriate threat potential, defined as a simple prediction or project loss. Furthermore, if the risk recurrence (e.g., depending on reliable information) is to be determined, the subject of potential risk and re-occurrence is estimated by the so-called effectiveness evaluations.

Moreover, it was observed that the true spectrum of project risks, the likelihood of hazards, impacts and projected duration are highly linked to uncertainty. In fact, it indicated that there are instabilities in the expense and profit calculations of each control option inside the project risk management framework. In case of an inadequate adaptation of the project risks mitigation plan, the weaknesses can result in losses. An estimation of the effectiveness or failure of the risk reduction plan is, therefore, necessary. It gives the technique of ensuring correctness a useful critique.

Effectiveness Evaluation: Results of the current approach are based on the effectiveness evaluation of the proposed approach. The effectiveness assessment is the measurement approach and confirms that the moderation targets were met. In spite of the fact that casual assessment and risk alleviation are made at a discreet time, the assessment technique should be continuously advanced. As mentioned previously, risk management has two common reasons for this method: recurrence method and estimation of chance. However, an estimation of chance is not the best method. Furthermore, the climate of a company could not be expected to remain ineffective. The structures, systems, services, employees, activities, and expectations of an organization can change over time. Opportunity estimation and risk relief should be revised intermittently to maintain the current condition.

VI. FUTURE TRENDS

At present, IT project risk management is more of a skill than a science, given that the entire strategies require calculation in amounts which are inherently questionable or difficult to evaluate. In addition, there is much more than one way of combining elements to perform a risk alleviation process. There are then a number of different approaches used today none of which are better certified than many others. Organizations choose a strategy for project-related risks to meet their needs. Within current strategies, there has been room for further calculating the precision and rising the rational assumption for risk management.

VII. CONCLUSION

The security of data is a progressive way of monitoring hazards. One might say that IT project risk management is essentially a groundwork for decision-making. The risk assessment method includes collecting the data to be used. The software development agency requires a managed risk control system and uses advanced techniques for risk mitigation. The evaluation of feasibility is the ongoing analysis of the IT development companies. While existing approaches can be modified, risk management definitely-serves to make companies competitive and sustainable. Organizations have multiple pressing requirements, protection and resource management are the secrets to deciding and legitimizing the distribution of scarce funds to security needs.

REFERENCES

1. Alberts, C., and Dorofee, A. (2002). Managing information security risks: the OCTAVE approach. Reading, MA: Addison Wesley.
2. Blakley, B., McDermott, E., and Geer, D. (2002). Information security is an information risk management. In proc. of ACM Workshop on New Security Paradigms (NSPW'01), 97-104.
3. Decker, R. (2001). Key elements of a risk management approach. GAO-02-150T, U.S. General Accounting Office.
4. Farahmand, F., Navathe, S., Sharp, G., and Enslow, P. (2003). Managing vulnerabilities of information systems to security incidents. In proc. of ACM 2nd International Conf. on Entertainment Computing (ICEC 2003), 348-354.
5. Geer, D., Hoo, K., and Jaquith, A. (2003). Information security: why the future belongs to the quants. IEEE Security and Privacy, 1(4), 24-32.
6. Gordon, L, and Loeb, M. (2002). The economics of information security investment. ACM Transactions on Information and System Security, 5, 438-457.
7. Hoo, K. S. (2000). How much is enough? A risk management approach to computer security. Retrieved October 25, 2006, from http://iis-db.stanford.edu/pubs/11900/soohoo.pdf.
8. McClure, S., Scambray, J., and Kurtz, G. (2001). Hacking Exposed: Network Security Secrets and Solutions, 3rd ed. New York, NY: Osborne/McGraw-Hill.
9. National Institute of Standards and Technology. (2002). Risk Management Guide for Information Technology Systems, special publication 800-30.
10. National Institute of Standards and Technology. (2003). Guideline on Network Security Testing, special publication 800-42.
11. Peltier, T. (2005). Information Security Risk Analysis, 2nd ed. New York, NY: Auerbach Publications.
12. Schneier, B. (2000). Secrets and Lies: Digital Security in a Networked World. New York, NY: John Wiley & Sons.
13. Vorster, A., and Labuschagne, L. (2005). A framework for comparing different information security risk analysis methodologies. In proc. of ACM Annual Research Conf. of the South African Institute of Computer Scientists and Information Technologists (SAICSIT 2005), 95-103.

AUTHORS PROFILE

Dr. Malaya Kumar Nayak, is an Entrepreneur and researcher with over 23 years leading the design, development and implementation of high-performance Executive Director with IT Buzz Ltd and U-Com Software Private Ltd. He has received M.S degree in ICT from Assumption University and PhD degree in Computer Science from Utkal University. He has published more than 25 research papers in National & International Conferences and Journals. His current research interests in project management and risk management.