International Journal of Scientific Research and Engineering Development-– Volume2 Issue 6, Nov-Dec 2019
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

RISK ANALYSIS IN INFORMATION TECHNOLOGY

Manishaben Jaiswal*

*Pursuing Ph.D. University of Cumberlands, Kentucky, USA
Email: mansha.p510@hotmail.com

----------**********----------

Abstract

Risk Analysis and Management is a key task administration exercise to make sure that the least variety of surprises take place whilst your task is underway. While we can by no means predict the future with certainty, we can follow an easy and streamlined threat administration procedure to predict the uncertainties in the tasks and reduce the incidence or have an effect on of these uncertainties. This improves the danger of profitable mission completion and reduces the penalties of these risks.This paper offers the structured Risk Management in information technology its scopes and resources. It also includes some tools which can help us in risk assessment and how it is impact on business impact analysis.

Keywords **— *Scope, Asset, Tools in risk assessment, Risk assessment finding, Business impact analysis***

----------**********----------

I. INTRODUCTION

Information technology is plays major role in business world, and risk is a sometimes a key of success. Like other field it has some risks factor. Most of the information technology risk include hardware and software failure, human error, spam, viruses and malicious attacks, as well as natural disasters such as fires, cyclones or floods. You can manage IT risks by completing a business risk assessment. The main sources of risk are operation risk, production risk, marketing risk, financial risk, legal risk, and human resource risks. Sometime risk is a key of success. In this paper I would like to introduce about some risk in information security and its scope, risk assessment and its business impact analyses

II. SCOPE

Risk is the uncertain events in the business environment, and risk assessment is an important part of the management. Changing in new inventory, method and employee can be a risk on a certain level. The project team must analyse risk to get success with changing in the environment. A certain level of risk assessment saves us from big losses in business. As the company grows up and changes in technology and methodology the new re-evaluation risk assessment is as follows.

A. Assets

Assets are the impartial value of the market. The company can determine the value via the replacement value of the asset. For example, if a laptop is stolen or fails then a new laptop price is $1,000. However, if we repair it in case of hardware replacement, operation system restore then cost downgraded up to $500. Save the asset using replacement value using recovery value. The example of the assets is data and information, personal, software and hardware asset and so on.

B. **People**

People or end-user cannot understand the reason for security control and restriction. They are responsible for managing the risk and perception of their account. The company provides a lock to keep the laptop at the desk, but some employee does not use this and leave the laptop on the desk and the result is lost or break the laptop.

C. **Process**

The new process will be more powerful in terms of authentication and authority. Although a user will take more than three attempts then the account will be a lock. Users must contact customer care to reactive their accounts. The user is not familiar with the process, then it causes a possibility of lost information.

D. **Technologies**

New technology is easy to manage at the client-side. Multiple data fetch the information from one server to another. We can use standby servers, cloud computing, and visualization which can help to create a hot site. We can share the data, files, and information and manage their permission using the cloud. It is the easy and cheapest way to share the data.

III. THE TOOLS USED TO CONDUCT THE RISK ASSESSMENT ARE AS FOLLOWS.

Currently, we have a team that can conduct the user issue according to their priority but as this technology is old, below are new approaches that can reduce the risk.

Fig 1 Risk assessment

A. **Training**

1. Give detail information to the employee about the new technique.
2. Training is only for some targeted people on the base of the review and disaster recovery plans.
3. Distribute responsibility among the employees.

B. **Testing**

1. Test the entire step in staging at the individual level using each possible phase.
2. Testing for each possibility of the plan during an emergency, for example, rebuild the database, back and restore.
3. Try to test new your changes from the different locations before you deploy on the site or production environment.Be ready for the alternate resources in case some process will fail.

C. **Exercise the work.**

1. Drill the new technology for regular time base on the scale.
2. Evaluate all possible functions in local and remote areas.

3. Check its damages and patches.

IV. RISK ASSESSMENT FINDING

Some of the threats as mention below can help in risk assessment.

1. A social engineer tracking employers relieving credentials.
2. Loss of examining and certifies the system with proper documentation.
3. Loss of system logs to identify the threat.
4. Hackers can hack the website due to lake of security.
5. The outside organization tries to track our company organization's details.
6. Spam calls from unauthorized users.
7. Natural disasters like electrical, heat or air-conditioning, fire you are not able to get due to virus attack.
8. Changes in location effects on the operation management system, sharing the files, match the profile.
9. Lost or stolen company assets like a laptop, monitor, and hard disk and so on.

V. BUSINESS IMPACT ANALYSIS

Business impact analysis is the large data collection process on the base of interviews, surveys, and meetings. According to our organization policy following steps, help on business impact.

Fig 2.0 Business impact analysis

1. You must have a good understanding of the environment including the customer and all transaction process automated and manual. Identify the group of people that can help to succeed in the issue. They can make sure the correct resources are used in the system. They can identify the system is critical or easy.
2. Focus on the critical function of the website. Focus on the remote data product and services. Check all the connectivity of the database server working properly or not. Analysis of your data and information on the base of loss and profit. If possible, find a possible recovery solution for it.
3. The main resource of the system like the internet, web application, database server, network connectivity must work properly. Use certified tools and technology for it.
4. Once you are able to find what the critical resources of your system, are then you can easily figure out maximum downtime. For example, for the webserver and database server, it is five minutes, for an email server. It is about eight hours.
5. If multiple issues come at the same time then select the priority level, if lower number with higher priority. Select the priority level like one, two or three. Generate a business analysis report for basic information documentation, system resources, and its critical roles and table connection for it.

VI. CONCLUSIONS

In conclusion, view of the variety of danger evaluation obligations and proficiencies in the federal government, it would be difficult, if no longer impossible, to produce a single particular technical instruction file that would be relevant to all federal agencies. New education that departs from mounted chance evaluation concepts and practices and is no longer supported by using the modern nation of the science is not likely to acquire the dreams referred to in the bulletin. Without baseline assessments of contemporary threat evaluation practices, needs, and capacities for enhancement in the federal agencies, neither OMB nor the

committee can make knowledgeable judgments on the types of preparation wished to attain the dreams set forth in the bulletin and the associated assets required to attain that end.

REFERENCES

[1] Bliss L. Tracy, Daniel Krewski, Jing Chen, Jan M. Zielinski, Kevin P. Brand & Dorothy Meyerhof (2006) Assessment and Management of Residential Radon Health Risks: A Report from the Health Canada Radon Workshop, Journal of Toxicology and Environmental Health, Part A, 69:7-8, 735-758, DOI: 10.1080/15287390500261281

[2] Harris, Anita 2005, VII. Discourses of desire as governmentality: young women, sexuality and the significance of safe spaces, Feminism, and Psychology, vol. 15, no. 1, pp. 39-43, DOI: 10.1177/0959353505049702

[3] Nadia Adnan, Shahrina Md Nordin, and Amir Noor Segmenting Paddy Farmer's Attitude and Behavior, Environmental and Agricultural Informatics, 10.4018/978-1-5225-9621-9.ch075, (1623-1648), (2020).

[4] Lamb SE, Jorstad-Stein EC, Hauer K, Becker C. Development of a common outcome data set for fall injury prevention trials: the prevention of falls network europe consensus. J Am Geriatr Soc. 2005;53:1618–22.

[5] Morris JC, Rubin EH, Morris EJ, Mandel SA. Senile dementia of the Alzheimer's type: an important risk factor for serious falls. J Gerontol. 1987;42:412–7

[6] S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," *IEEE Electron Device Lett.*, vol. 20, pp. 569–571, Nov. 1999.

[7] M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "Highresolution fiber distributed measurements with coherent OFDR," in *Proc. ECOC'00*, 2000, paper 11.3.4, p. 109.

[8] R. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, "High-speed digital-to-RF converter," U.S. Patent 5 668 842, Sept. 16, 1997.

[9] A. Karnik, "Performance of TCP congestion control with rate feedback:TCP/ABR and rate adaptive TCP/IP," M. Eng. thesis, Indian Institute ofScience, Bangalore, India, Jan. 1999.

[10] J. Padhye, V. Firoiu, and D. Towsley, "A stochastic model of TCP Renocongestion avoidance and control," Univ. of Massachusetts, Amherst,MA, CMPSCI Tech. Rep. 99-02, 1999.

[11] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*,IEEE Std. 802.11, 1997.

