Risk Management in the IT Department

Rahul Reddy Nadikattu*

Department of Information Technology, University of the Cumberlands,
6178 College Station Drive, Williamsburg, KY 40769, United States.

ABSTRACT

The proposed paper summarizes the information on risk management based on the perusal of scientific literatures. The study focuses on the critical areas of a typical Information Technology that has narrowed down for cyberattacks to four key assets that are presently vulnerable to threats. The four identified assets include the SQL Database, the company's website, Data Centers, and Servers. The study also focuses on the business continuity plan, along with the disaster recovery plan. The study highlights the structured and active management of risk in the IT department and significantly provides the standardized process and its manageable strategies.

Keywords: *Risk management, IT Department, Risk Factors, Risk Processes, Servers, Data Centers, Disaster Recovery Plan.*

1. INTRODUCTION

Technology is impacting how several organizations conduct business in a growing market. Due to the occurrence of these changes, a challenge has been faced by the industries for developing technical approaches for simplifying every task that is more contextual, more secure, and faster. Companies need to change, along with adapting to existing changing trends in technology, which endure in the future. To come across any objective in any aspiring business, putting in place a strategic plan is essential for working efficiently. With the implementation of the appropriate systems and strategies, the costs have outweighed the benefits, leading to increased profit margins, enhanced efficiency, and improved productivity. Created new essential strategic goals that must mirror the company's commitments and mission of this research paper focuses on applying a risk management plan in the Information Technology sector, defining the process of risk management that has to implement throughout the organization's life. It has aimed at focusing on risk management strategies. The paper focussed on four assets that exist in any organization's IT department. These assets include the SQL Database, Company Website, Servers, and Data Center. The paper focussed on the business continuity plan, along with the disaster recovery plan. The strategies to mitigate the risk and mitigation plan has presented in this paper. These strategies assisted organizations, particularly in the United States. With the implementation of strategies, overall efficiency, and productivity of the organization has increased, and it boosted the organization's earnings.

2. SCIENTIFIC UPDATED REPORTS

As per Kozak-Holland (2005), the IT project is characterized by material and human resources, demand, risk, scope, innovation, and the essential time for execution [1]. Similarly, Goodwin (2002) believes that every project, also an IT venture, is burdened with risk. Risk has been defined by Goodwin (2002) as a phenomenon or activity's occurrence's probability degree that might have a positive or negative effect on the entire project's course. For the risk, one most significant characteristic is the likelihood of assessing its probability, along with determining its impact on the whole project. With the help of this, the manager of the project can influence or manage the risk actively [2]. Further, as per Keyes (2008), the risk is the most critical process in managing the project [3]. In the study conducted by Kendrick, (2015) reported that without risk, there is no venture [4]. And according to Marcelino-Sádaba, Pérez-Ezcurdia, Lazcano & Villanueva, (2014) perceived the project's threat as the probability's measure and failure to achieve the goals of the project. In the subject's literature, attention has drawn to fact risk concerns to loss, along with the chances of achieving better outcomes in the project, or at its stage [5]. Also, study of Well-Stam, Lindenaar & van Kinderen (2004) referred to the risk management as the principles' regular usage, the process and approach of identification of assessment of risk, and planning, along with the implementation of actions that address the threat. An environment in which one can make proactive decisions [6].

Moreover, Raydugin (2013) defined risk management as a method of power, focusing on identifying and controlling events or areas that can adversely change. For management, it is an essential element grounded on a general approach to risk, to be precise, the risk is a collection of numerous diverse factors [7]. Four steps were distinguished by Conrow (2003) in the risk management process in projects, which comprise: identification of risk, analysis of risk, steering of risk, and control of risk [8].

2.1. Process of Risk Management

According to Tohidi (2011), in the entire process of risk management, defined risk identification as the first phase. The entire team of the project in this phase needs to carry out a joint discussion. The outcome of this discussion needs to be a sign of the risk types in the existing undertaking. The study also suggests that organizing a minimum of one meeting dedicated issues related to project risk. It is easy in this way to make the project team's members conscious of the risk identification phase's significance [9]. Identification of risk as per Kishk & Ukaga (2008) consists of the definition of possible threats or risk factors in other words [10]. This step's primary goal, as per Segal (2011), is the detection of threats that might limit or even prevent the likelihood of attaining the opportunities and goals that may result in improved outcomes [11].

The analysis of risk is the next step in the process of risk management is that as per PMI (2013) needs to be split into 2 phases, quantitative and qualitative risk analysis. Qualitative risk analysis is related to the hierarchy of risk that heads their further activities or research associated with them and implemented by referencing and assessing their consequences and probability of occurrence. For this phase, the project manager's key benefit is reducing uncertainty level and focusing on a particular project's most significant risks. Quantitative analysis of risk is related to the numerical evaluation of the identified risks' impact on the customarily accepted objectives of the undertakings. This process's key benefit is the quantitative information acquisition on hazards that assist in supporting the decision-making decision, focusing on minimizing the entire undertaking's uncertainty. There is one more approach to risk analysis that treats this phase as a single phase. It indicates two factors that define the real risk: the occurrence's probability and occurrence's consequences [12]. According to Webb (2003) [13] and PMI (2013) [12] differentiate the four tactics of handling with risk:

- Risk acceptance and its possible impacts in the form in which it takes place: This method needs to use with a low blow for events.
- Eliminating or decreasing the events' probability or their impacts (or both). With the changing of one dimension of the project out of four sizes, it becomes possible: quality, schedule, budget, or scope. This process best works with predictable risk factors.
- Transferring of risk with the help of including subcontractors, insurance, or guarantees*:* One can manage risk in this way. Though, it is essential to confirm if the insurance is not more costly as compared to this risk's effects.
- Establishing future provisions and activities' plans that would be used in the event of triggering risk: The probability is not affected by such actions, but they minimize the potential impacts. One can apply such a strategy, for instance, to natural disasters and other volatile events that can take place in the coming years.

As per the study of Burk (1999), four strategies for managing risk, though he presented them in a bit different way: risk avoidance, hazard mitigation, threats transferring, and threats accepting [14]. The method of planning risk response is the third step in the process of project risk management. In this phase, as per Pritchard (2001), related to the actions' definition using which issues must be resolved, which is associated with the risks' particular types that have been analyzed and identified in preceding phases [15].

In the process mentioned above, the last phase is to associate with risk control. This phase comprises the hazards' ongoing monitoring throughout the project's implementation and responding with the threats' emergence as planned. It is necessary during this process to consider the following principles [16].

- There is a variable risk - the threats' occurrence likelihood and their outcomes might alter with time.
- Numerous strategies could be used for managing risk efficiently.
- There is no need to give up the management of risk for unforeseen events and general uncertainty.

3. METHODOLOGY

Since the Information Technology department within any organization deals with the organization's critical data, it is essential to focus on any cyber-attacks that can take place in any organization. Furthermore, it is necessary

to evaluate the risk associated with the assets that can be impacted by different cyber-attacks. The areas of a typical Information Technology department has narrowed down for cyberattacks to four key assets that are vulnerable to threats presently. The four identified assets include the SQL Database, the website of the company, Data Centers, and Servers. The chart below is providing the actual assessment of risk for the organization (Table 1).

Table 1: Organization of risk management.

Vulnerable Assets or Operations	**Hazards**	**Scenarios**	**Mitigation Opportunities**	**High, Medium, Low Probability**
Database of SQL	For specifically SQL, injection attacks are used by the hackers use	Every information related to the clients can be stolen by the hackers	● Creating queries for distinguishing data vs. codes. ● Setup privileges of user to the least levels but enables high privileges to those who need it absolutely.	Medium
Website of the Company	Scripting techniques are used by the hackers use for creating a fake website of the company	The personal information of the clients can be stolen by the hackers	● Within a website, there is a need for creating an escape framework that will assist in avoiding such website scripts.	High
Servers	Unpatched vulnerabilities can be exploited by hackers.	The vulnerabilities are used by the hackers for crashing the network, along with stealing the information	● There is a need for performing assessments for vulnerability. ● Patching every vulnerability. ● Monitoring the servers with IPS and IDS.	Medium
Data Center	The Datacenter can catch fire	Data loss and damage to property can take place due to fire	There must be a substitute location that at least has the updated backed up data. Install environmental alerting system and fire suppression system	Low

4. DISCUSSION

4.1. SQL Database

The first venerable asset is the Database of SQL. For such a purchase, the possible type of hazard would include threats from hackers that penetrate the database with the help of an injection attack precisely for SQL. There are high chances that the hacker can steal all client information from the organization while exploiting the database with particular malware codes. If succeeded, the impact of such an attack would be considered higher on individuals since the personal information of clients and employees would be compromised. As per Burnette (2017), the impact of such attacks would consider higher on the property as this would become the reason for a significant monetary burden on the organization [17].

Similarly, the effect of such attacks would be regarded as a medium on the environment and operations as such attacks would not wholly immobilize the organization from performing its day to day tasks. Still, it would make things harder in the process, making individuals struggling to strengthen the structure. For such an attack, the impact would consider medium because this would not destroy the company's reputation but become the reason for the organization to put all of its efforts into regaining the trust of customers and employees. Because of every impact mentioned above, the medium-high rating is the overall hazard as the property and people would be affecting significantly.

4.2.Mitigation

A solution that would assist in preventing such attacks is to creating certain queries that differentiate the difference in the middle of data and malicious codes that must be there [18]. One more strategy for helping in mitigating such attacks is by setting specific privileges. With this, it would indicate that there is the lowest possible privilege for every employee that is merely sufficient for conducting the work of employees, along with having a particular set of authentications for individuals who need higher benefits. A hacker seeking to attack SQL on an organization only has a 50/50 chance of success, and this is the crucial reason to declare this probability as the medium.

4.3.Company Website

The website of the organization is the next asset at risk. The website enables the customers to register the appointments online. The possible chance against the site would include the threats from hackers who use some cross-website scripting to modify the limitations within the internet browser to direct the customer to the fake website. In the case of any organization, the hacker can steal all the login information of the clients for infiltrating their personal computers to do whatever they want to the customer. In this case, the clients would have doubts about the organization's website, and they could avoid using the site.

The impact of such an attack would be considered high on people as the personal information of the customers would be stolen and exploited. The effect of such an attack would be regarded as the medium on the property as this could cause sure clients not to register on the company's website anymore and could hurt the organization's goodwill. The impact of such an attack would be considered low on operations as there would be minimal impact of such a threat on the organization's operations. The effect of such an attack would be regarded as high on the environment as the website would have to be closed entirely until the rectification of the issue. Based on all these impacts, the overall risk rate as a medium-high.

4.4. Mitigation

A solution that would assist in mitigating such attacks would be creating a framework within the website's coding that would automatically help prevent cross-website scripting from being used. Such attack risks would have a lower probability as cross-website scripting does not take place every often. .

4.5. Servers

The next asset at risk would be the servers of the organization. For an organization, this is a physical aspect that is important for the organization's day-to-day operations. The possible risk such an asset would be a threat from a hacker misusing vulnerabilities of the server that are unknown to the organizations and has no patch yet. These unpatched vulnerabilities can be used by the hacker who can exploit them and attack the servers causing it to crash the network entirely and stealing.

The impact of such an attack would be considered high on people as all the personal information of clients, management, and employees would be compromised. Such an attack would be regarded as high on the property as every server would possibly be left with viruses and must reimage completely. Such an attack would be considered

high on operations as these servers control the daily operations of the company, along with the environment that would create a complete operational loss, along with an entirely compromised infrastructure if every server went down. The impact of such an attack would be considered high on the entity as this would cause the organization to stop taking appointments, which can lead to revenue loss until the system is up again. Because of all these impacts, the overall risk is rated as high.

4.6. Mitigation

A solution that would assist in mitigating such attacks would be to occasionally perform assessments for vulnerabilities to find active or newer vulnerabilities on the servers. The known vulnerabilities have patched after the completion of the analysis. Also, there is a need for implementing Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) for preventing attacks similar to this. In my opinion, such attacks would have a medium probability is almost expected that such an organization has few, if any, unpatched vulnerabilities.

4.7. Data Center

The organization's data center is a vulnerable asset. This center aimed at placing the backup of the organization's entire data. The possible type of risk for the data center would include the fire in the data center. The data center can catch fire, causing a total data loss and damaging the building externally and internally.

The impact of the attack would be regarded as a medium on people as this building would be minimally operated. It is improbable that individuals have trapped in case the building caught fire. Such an attack's impact would be regarded as high on the environment and property, as there would be great damage to the equipment and the stuff that goes with the building. The impact of such an attack would be considered medium on operations as the fire would not straight become the reason for stopping the current processes. Instead, it would cause long working hours and more hardship for restoring the data lost. Such an attack would be considered low on the entity as the company would have insurance covering the affected property and equipment. Due to all these effects, there is an overall medium rating risk as the data center's actual building would be the only one affected by such a disaster.

4.8. Mitigation

A solution for preventing such attacks is to have a substitute data center if such a disaster occurs. The substitute data center would have the same means and equipment as the affected location. Also, there must be a system of fire suppression, along with a network of environmental alerting installed for mitigating such attacks.

4.9. Business Continuity Plan

Business continuity can be well-thought-out as the activities performance required for keeping an organization up and running through disruption or displacement of usual operation. The actual plan emphasizes the processes and people that result in profitability. It is a rigorous and comprehensive compilation of information and methods maintained and ready for use in a catastrophic event.

The Business Continuity Plan aimed at ensuring that the organization has a thorough process implemented if any disaster occurs within its infrastructure. Business Continuity must cover power, equipment, or failure of the application and corruption of the database [19].

The Business Continuity Plan implemented by the organization includes a Risk Assessment, Business Impact Analysis, Resumption Strategies, Incident Response, and Disaster Recover [19]. Risk Assessment comprises a table that keeps assets at risk within the organization and how these risks impact the organization. For an organization, the Resumption Strategies focused more on backup options and recovery for organizing in case of occurrence of any disaster. For an organization, the implemented incidents response is where a specialist's team step-by-step respond to all and any incident taking place in the organization.

For an organization, the Resumption Strategies focused more on backup options and recovery for organizing in case of occurrence of any disaster. For an organization, the implemented incidents response is where a specialist's team step-by-step respond to all and any incident taking place in the organization. For an organization, disaster recovery would be in which the step-by-step process of reintegrating, restoring, and repairing the primary location of the organization back to normal operations after a disaster.

4.10. Disaster Recovery Plan

This plan is required by the organization to determine the recovery time to minimize the maximum downtime amount post-disaster. To meet this requirement, the organization needs to have a replicated infrastructure of data at an alternative location for ensuring the continuousness of the operations. The process of disaster recovery immediately occurs after a disaster to the primary facility, along with relocating an alternative site for sustaining the

business continuity [20]. It is required by this plan that the secondary location is appropriate sufficiently for the data to live that can only take place by hardware and software, connectivity of the network, and security. An effective strategy of disaster recovery is merely contingent on the planning, determining the elements that are well-thought-out as critical to the mission, and generating the appropriate order of return, along with a way for accomplishing successful tests [21]. The Response Phase indicates that the Response process starts right after the DRP is initiated. When a disaster occurs in the organization, the response can be a matter of misuse of the confidential date; hence, in this stage, the duties must be executed by the Response team as safely and quickly as possible [22].

The Recovery Phase indicates that after the response phase, the recovery phase starts where the organization conducts its repairs, move the operations to the alternative location, and backing up the data to prevent further losses.

In the Resumption Phase, the business would recover entirely, along with resuming the everyday operations as it starts the restoration phase. It is the phase where the repairs completed to the system of the organization. In this phase, the organization regain its sense of normality and move on from the disaster.

5. CONCLUSION

Technology is impacting how numerous organizations conduct business in a growing market. Since the Information Technology department within any organization deals with the critical data of the organization, it is essential to focus on any cyber-attacks that can take place in any organization. The essential areas of a typical Information Technology department had narrowed down for cyberattacks to four key assets (SQL Database, Website of Company, Servers, and Data Center) that are vulnerable to threats presently. Significantly, there is a standardized process of risk management, and it has managed actively. With the implementation of proper risk management, the overall efficiency and productivity of the organization would increase, and it boosts the earnings of the organizations.

6. REFERENCES

[1] Kozak-Holland, M. (2005). Titanic lessons for IT projects. Multi-Media Publications Inc.

[2] Goodwin, S. (2002). Troubled IT projects: prevention and turnaround [Book Review]. Engineering Management Journal, *12*(2), 54-54 pp.

[3] Keyes, J. (2008). Leading IT Projects*:* The IT Manager's Guide. CRC Press.

[4] Kendrick, T. (2015). Identifying and managing project risk*:* essential tools for failure proofing your project. Amazon.

[5] Marcelino-Sádaba, S., Pérez-Ezcurdia, A., Lazcano, A. M. E. & Villanueva, P. (2014). Project risk management methodology for small firms. International journal of project management, *32*(2), 327-34 pp.

[6] Van Well-Stam, D., Lindenaar, F., & van Kinderen, S. (2004). Project risk management: An essential tool for managing and controlling projects. Kogan Page Publishers

[7] Raydugin, Y. (2013). Project risk management*:* Essential methods for project teams and decision-makers. John Wiley & Sons.

[8] Conrow, E. H. (2003). Effective risk management: Some keys to success. Aiaa.

[9] Tohidi, H. (2011). The Role of Risk Management in IT systems of organizations. Procedia Computer Science, *3*, 881-887 pp.

[10] Kishk, M., & Ukaga, C. (2008). The impact of effective risk management on project success. Retrieved from https://rgu-repository.worktribe.com/output/248394/the-impact-of-effective-risk-management-on-project-success.

[11] Segal, S. (2011). The corporate value of enterprise risk management. Hoboken (NJ): Wiley.

[12] PMI (2013). A Guide to the Project Management Body of Knowledge, 5th ed. Project Management Institute, 541 pp

[13] Webb, A. (2003). The project manager's guide to handling risk. Gower Publishing, Ltd. 231 pp.

[14] Burk, R. (1999). Project management. Planning and Control Techniques. John Wiley & Sons LTD, Chichester, New York, 374 pp.

[15] Pritchard, C. L. (2001). Risk Management, Concepts, and Guidance, ESI International, 346 pp.

[16] Förster, C. (2008). Risikomanagement in Web-Projekten [Risk management in Web-Projekts]. Technical University of Munich, Munich, 278 pp.

[17] Brunette (2017), Wichers, D. (2018, February 06). *SQL* Injection Prevention Cheat Sheet. Retrieved from https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet
[18] Wichers, D. (2018, February 06). *SQL* Injection Prevention Cheat Sheet. Retrieved from https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet
[19] Fried, S. (2001). Information Security: The Big Picture – Part IV," Information Security KickStart Highlights, SANS GIAC. Retrieved from http://www.sans.org/reading-room/whitepapers/recovery/introduction-business-continuity-planning-559
[20] Jorrigala, V. (2017). Business Continuity and Disaster Recovery Plan for Information Security. Retrieved from https://pdfs.semanticscholar.org/59b5/fc8f6be0de6106dde57e479d383a9c6781ee.pdf. 42 pp.
[21] Gregory, P. H. (2007). *IT* disaster recovery on planning for dummies. John Wiley & Sons. 198 pp.
[22] Whitman, M. E., Mattord, H. J., & Green, A. (2013). Principles of incident response and disaster recovery. Cengage Learning. 423 pp