**Risk Management Plan**

**<Risk Analysis plan>**

**Date**

# 2/18/2017

**Table of Contents**

[Introduction 3](#_Toc332278598)

[Threats and vunerabilties in this case 4](#_Toc332278603)

[Chain of Breach Events 4](#_Toc332278599)

[Table of Asset Effected and Classification 5](#_Toc332278600)

[Risk Mitigation and Avoidance 7](#_Toc332278601)

[Action Taken on Sonja 8](#_Toc332278602)

# Introduction

Here is the case, we found one of our very important and big competitor was been bankrupt, and which made our organization to start increasing name and fame to it’s peak. We increased our support functionality from 5 days working by giving holidays on the mandatory days to working on 24 by 7 shifts. We are now supposed to ensure that whenever if there is a support request raised in the organization to IT Helpdesk Department, we are expected to close the ticket within less span than anticipated. The tickets which would generally raise would be of account lock, forgotten passwords, also we communicate with user as necessary on desired. One fine day, one of the support staff from IT Helpdesk has downloaded a movie named as Starswars in the organization system from a external site cited as “the pirate bay” in one of our office computer. Where After few days people started saying system running became slow, and where after a basic analysis and research by our risk analysis team, we had found that botnet installations in all our company system, and we find a keylogger for this in our IT HelpDesk in one of the machine. So for this we are providing the report on below mentioned points by our CEO.   
  
Consider this event in high risk management by the analysis by our risk analysis team, answering the questions.

1. Evaluate what threats and vulnerabilities allowed this situation to occur.  What is the chain of breach events?   
     
     
   Threats and Vulnerabilities.

The top high probability and high impact threats and vulnerabilities to this project are:

**Allowance of opening of External site threats of virus and system and network collapse**

By allowing the user to open the external site would make them to get access to have access to all sites, which means they are eligible for accepting bots and virus and where there are special bots which are not identified by our anti virus or firewall. If this run in our network, then it would impact total company network database and network, which is not authorized to accept and follow the steps as mentioned in the external site.

**Opening the gate for black hats for our system internal records.**

These would create problem for and give a gap for internal records get established to black hat people, where it get misused by the people, and also it can mis placed which would get value of the organization gets in place and we might loss our name and fame, where it would create huge problem in criminal reference, and would make legal penalties on the organization if the information is misused and got leaked, and woukd impact with HR rules.

**Training of User, User are tend to be a risk with company system information, and there job.**

User would be considered to be always a biggest asset and also biggest problem in some of the scenario, this does not mean that we are having some kind of doubt on people, and so in order to make the working functionality smoothly, so we would make effectively help from the user and trsut would be considered as a very important thing among all the people, and in this kind of scenario, we would like to have user given with proper authorization and training and where training department, and HR Department inputs are always required, and knowing as a user what are they supposed to do in terms of making a effective running as a organization.   
  
  
While explaining the three important factors, We had given the series of breaches which would be considered as high level security breach, and would be decided on the review of CEO and other higher management, Respective of IT , Networking ,Training , HR Departments are the series department which are involved in this scenario, respective this kind of scenario should not repeat .

# Risk Management Approach

This section provides a general description for the approach taken to identify and manage the risks associated with the project. It should be a short paragraph or two summarizing the approach to risk management on this project.

The approach we have taken to manage risks for this project included a methodical process by which the project team identified, scored, and ranked the various risks. The most likely and highest impact risks were added to the project schedule to ensure that the assigned risk managers take the necessary steps to implement the mitigation response at the appropriate time during the schedule. Risk managers will provide status updates on their assigned risks in the bi-weekly project team meetings, but only when the meetings include their risk’s planned timeframe. Upon the completion of the project, during the closing process, the project manager will analyze each risk as well as the risk management process. Based on this analysis, the project manager will identify any improvements that can be made to the risk management process for future projects. These improvements will be captured as part of the lessons learned knowledge base.

**2. Table for Asset Affected, Threat agent, Threat action, Vulnerability used.** :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S.no | Asset Effected | Threat Agent | Threat Action | Vunerability Used |
| 1 | System | IT | Authorization, Limited | bot |
| 2 | Network | IT | Firewall, Restricted | bot |
| 3 | User | HR, Training | Restricted | Virus, User |
| 4 | Records | Legal Terms | Values, Restricted | Bot , Virus, user |
| 5 | Finance | Finance | Restricted, Confidential | Virus, User |

3. List the actions the company must take to prevent such events in the future. (10 points)

# Risk Identification

This section explains the process by which the risks associated with this project were identified. It should describe the method(s) for how the project team identified risks, the format in which risks are recorded, and the forum in which this process was conducted. Typical methods of identifying risks are expert interview, review historical information from similar projects and conducting a risk assessment meeting with the project team and key stakeholders.

For this project, risk identification was conducted in the initial project risk assessment meeting. The method used by the project team to identify risks was the Crawford Slip method. The project manager chaired the risk assessment meeting and distributed notepads to each member of the team and allowed 10 minutes for all team members to record as many risks as possible.

**Expert Interview**

Two Expert Interviews were held for this project. The interviews revealed several risks which were then mitigated by making changes to the project plan. The remaining risks are included in the Risk Register.

**Risk Assessment Meeting**

A risk assessment meeting was held with key team members and stakeholders. The risks identified during this meeting were added to the project plan and Risk Register.

**Historical Review of Similar Projects**

The project team reviewed the history of similar projects in order to determine the most common risks and the strategies used to mitigate those risks.

# Risk Qualification and Prioritization

Once risks are identified it is important to determine the probability and impact of each risk in order to allow the project manager to prioritize the risk avoidance and mitigation strategy. Risks which are more likely to occur and have a significant impact on the project will be the highest priority risks while those which are more unlikely or have a low impact will be a much lower priority. This is usually done with a probability – impact matrix. This section explains risks were qualified and prioritized for this project. For more information on how to qualify and prioritize risks refer to our ***Risk Assessment Meeting Guide.***

In order to determine the severity of the risks identified by the team, a probability and impact factor was assigned to each risk. This process allowed the project manager to prioritize risks based upon the effect they may have on the project. The project manager utilized a probability-impact matrix to facilitate the team in moving each risk to the appropriate place on the chart.

Once the risks were assigned a probability and impact and placed in the appropriate position on the chart, the recorder captured the finished product and the project manager moved the process on to the next step: risk mitigation/avoidance planning.

# Risk Monitoring

This section should discuss how the risks in the project will be actively monitored. One effective way to monitor project risks is to add those risks with the highest scores to the project schedule with an assigned risk manager. This allows the project manager to see when these risks need to be monitored more closely and when to expect the risk manager to provide status updates at the bi-weekly project team meetings. The key to risk monitoring is to ensure that it is continuous throughout the life of the project and includes the identification of trigger conditions for each risk and thorough documentation of the process.

The most likely and greatest impact risks have been added to the project plan to ensure that they are monitored during the time the project is exposed to each risk. At the appropriate time in the project schedule a Risk Manager is assigned to each risk. During the bi-weekly project team meeting the Risk Manager for each risk will discuss the status of that risk; however, only risks which fall in the current time period will be discussed. Risk monitoring will be a continuous process throughout the life of this project. As risks approach on the project schedule the project manager will ensure that the appropriate risk manager provides the necessary status updates which include the risk status, identification of trigger conditions, and the documentation of the results of the risk response.

# Risk Mitigation and Avoidance

Once risks have been qualified, the team must determine how to address those risks which have the greatest potential probability and impact on the project. This section explains the considerations which must be made and the options available to the project manager in managing these risks.

The project manager has led the project team in developing responses to each identified risk. As more risks are identified, they will be qualified and the team will develop avoidance and mitigation strategies. These risks will also be added to the Risk Register and the project plan to ensure they are monitored at the appropriate times and are responded to accordingly.

The risks for this project will be managed and controlled within the constraints of time, scope, and cost. All identified risks will be evaluated in order to determine how they affect this triple constraint. The project manager, with the assistance of the project team, will determine the best way to respond to each risk to ensure compliance with these constraints.

In extreme cases it may be necessary to allow flexibility to one of the project’s constraints. Only one of the constraints for this project allows for flexibility as a last resort. If necessary, funding may be added to the project to allow for more resources in order to meet the time (schedule) and scope constraints. Time and scope are firm constraints and allow for no flexibility. Again, the cost constraint is flexible only in extreme cases where no other risk avoidance or mitigation strategy will work.

**Risk Register**

Every project must maintain a risk register in order to track risks and associated mitigation strategies. This section describes the risk register criteria as well as where the risk register is maintained and how these risks are tracked in the project schedule.

The Risk Register for this project is a log of all identified risks, their probability and impact to the project, the category they belong to, mitigation strategy, and when the risk will occur. The register was created through the initial project risk management meeting led by the project manager. During this meeting, the project team identified and categorized each risk. Additionally, the team assigned each risk a score based on the probability of it occurring and the impact it could potentially have. The Risk Register also contains the mitigation strategy for each risk as well as when the risk is likely to occur.

Based on the identified risks and timeframes in the risk register, each risk has been added to the project plan. At the appropriate time in the plan—prior to when the risk is most likely to occur—the project manager will assign a risk manager to ensure adherence to the agreed upon mitigation strategy. The each risk manager will provide the status of their assigned risk at the bi-weekly project team meeting for their risk’s planned timeframe.

The Risk Register will be maintained as an appendix to this Risk Management Plan.

4. Recommend what actions to pursue with Sonja. (10 points)  
  
In this Scenario, We as a team identified as a high level security breach made by technical assistant by allowing an external bot our network, so and we would request to fire the person from the organization, but how ever the review or decision would be taken by CEO and higher management, but it is our suggestion from risk management team, and if we keep a strict rule on this kind, then there is a no possibility of this kind of this situation would repeat, and it would become a common rule, and people would get a strong order and fear of there respective job and we can protect our organization name and fame.