Experiment No. 10

Aim: To prepare RMMM plan for the Vibez (social media) software

Theory:

Planning the risk management

The proactive strategy for risk estimation is used which helps us in identifying the possible threats that can occur during the project well in advance. Accordingly, steps to avoid, monitor and manage the risk are to be carried out and noted down in the form of RMMM plan.

Example:

THE RMMM PLAN

A risk management strategy can be included in the software project plan or the risk management steps can be organized into a separate Risk Mitigation, Monitoring and Management Plan. The RMMM plan documents all work performed as part of risk analysis and is used by the project manager as part of the overall project plan. Some software teams do not develop a formal RMMM document. Rather, each risk is documented individually using a risk information sheet (RIS) . In most cases, the RIS is maintained using a database system, so that creation and information entry, priority ordering, searches, and other analysis may be accomplished easily.

Once RMMM has been documented and the project has begun, risk mitigation and monitoring steps commence. As we have already discussed, risk mitigation is a problem avoidance activity. Risk monitoring is a project tracking activity with three primary objectives:

(1) to assess whether predicted risks do, in fact, occur

(2) to ensure that risk aversion steps defined for the risk are being properly applied

(3) to collect information that can be used for future risk analysis. In many cases, the problems that occur during a project can be traced to more than one risk. Another job of risk monitoring is to attempt to allocate origin (what risk(s) caused which problems throughout the project).

Identifying Risks:

Risk ID	Risk Summary	Probability	Impact	Risk Exposure
1	Data Leak	50%	1	Rs. 70,000/month
2	Server/Application Hacked	60%	1	Rs. 20,000/month
3	Financial Loss Due To Malware	20%	2	Rs. 20,000/month
4	Violation Of Privacy	40%	2	Rs. 16,000/month

Impact:

1 – Catastrophic
2 – Critical
3 – Marginal
4 – Negligible

Sorting the risks on the basis of their risk exposure:

Risk ID	Risk Summary	Probability	Impact	Risk Exposure
1	Data Leak	50%	1	Rs. 70,000/month
2	Server/Application Hacked	60%	1	Rs. 20,000/month
3	Financial Loss Due To Malware	20%	2	Rs. 20,000/month
4	Violation Of Privacy	40%	2	Rs. 16,000/month

Impact:

1 – Catastrophic
2 – Critical
3 – Marginal
4 – Negligible

Risk Exposure:

Risk:

Wrong Accusation
The platform is meant to be used by netizens to upload their photos and videos and take part in various activities and collaborations so that people can get to know each other. Data leak is causing this private data to be leaked to various online hackers and competitiors

Risk Probability: 50%

Risk Impact:

The risk impact would be catastrophic as this would defeat the whole purpose of developing such an application. If the number of the cases of wrong accusation increases, this will lead to the wastage of time and the resources.

Risk Information Sheet:

<table>
<tr><td>Risk ID: 1</td><td>Date: 02/10/2023</td><td>Probability: 50%</td><td>Impact: Catastrophic</td></tr>
<tr><td colspan="4">Description:
The platform is meant to be used by netizens to upload their photos and videos and take part in various activities and collaborations so that people can get to know each other. Data leak is causing this private data to be leaked to various online hackers and competitors</td></tr>
<tr><td colspan="4">Refinement/Context:
To solve the problem of data leak we need to ensure that data remains secure and no fake accounts are made to steal this data .</td></tr>
<tr><td colspan="4">Mitigation/Monitoring:
1. Higher security should be maintained
2. Accounts of such users will be blocked.</td></tr>
<tr><td colspan="4">Management:
RE computed to be Rs. 50,000 per month.</td></tr>
<tr><td colspan="4">Current Status:
Mitigation steps to be initiated.</td></tr>
<tr><td colspan="2">Originator: Vivaan Mansukhani</td><td colspan="2">Assigned: Arnav Malvia</td></tr>
</table>

Risk Exposure:

Risk:
If the system gates hacked then all the data of the company and it's users gets compromised and then people are at risk of getting exposed.

Risk Probability: 60%

Risk Impact:

The risk impact would be catastrophic as it would make it impossible for the company to get back the stolen data and anything can be done using it.

Risk Exposure:

RE = 0.6 x Rs. 33,333 = Rs. 20,000/month.

Risk Information Sheet:

Risk ID: 2	Date: 2/10/2023	Probability: 60%	Impact: Catastrophic
Description: If the system gates hacked then all the data of the company and it's users gets compromised and then people are at risk of getting exposed.			
Refinement/Context: Sub condition 1: The risk impact would be catastrophic as it would make it impossible for the company to get back the stolen data and anything can be done using it.			
Mitigation/Monitoring: 1. Usage of better security 2. Training a better algorithm for data 3. Ensureing two factor verification			
Management: RE computed to be Rs. 20,000 per month.			
Current Status: Mitigation steps to be initiated.			
Originator: Arnav Malvia		Assigned: Rishab mandal	

Risk Exposure:

Risk:
Currently malware cannot be detected by traditional way based anti-malware tools due to their polymorphic and/or metamorphic nature. Here we have improvised a current detection technique of malware based on mining Application Programming Interface (API) calls and developed the first public dataset to promote malware research.

Risk Probability: 20%

Risk Impact:

Malware can cause significant loss and incur substantial costs to organizations. The desire to avoid detection coupled with often lucrative nature of malware development means that there is a high probability that new malware is developed it will likely utilise unknown techniques. Though it can be mitigated by using some firewalls to prevent malware attacks via input details.

Risk Exposure:

RE = 0.3 x Rs. 66,666 = Rs. 20,000/month.

Risk Information Sheet:

<table>
<tr><td>Risk ID: 3</td><td>Date: 02/10/2023</td><td>Probability: 20%</td><td>Impact: Critical</td></tr>
<tr><td colspan="4">Description:
Malware attacks can cause significant loss to the organization and can lead to several hours of downtime. Downtime will reduce revenue and would also disappoint the users of the application.
It may also lead to leakage of sensitive data of the users.</td></tr>
<tr><td colspan="4">Refinement/Context:
Sub condition 1:
Malware can slow down a user’s computer and has the ability to crash some websites. It can infect your computer and use it as a server to broadcast various files or attacks.

Sub condition 2:
Malware can send emails you did not write getting you or your company in trouble which can result in the company's huge loss. To minimize these attacks firewalls are used.</td></tr>
<tr><td colspan="4">Mitigation/Monitoring:
1. Use of antivirus, firewalls and anti-malware software.
2. Monitoring should be in place to verify the security state of: a Update your operating system, browsers, and plugins. b Read the emails with eagle eyes.
c Don’t believe cold callers. d
Don’t call fake tech support.
e Make sure you’re on a secure connection.
3. Use strong passwords or password managers.</td></tr>
<tr><td colspan="4">Management:
RE computed to be Rs. 20,000 per month.</td></tr>
<tr><td colspan="4">Current Status:
Mitigation steps to be initiated.</td></tr>
<tr><td colspan="2">Originator: Vivaan Mansukhani</td><td colspan="2">Assigned: Rishab Mandal</td></tr>
</table>

Risk Exposure:

Risk:

Violation of Privacy.

In today’s world, data is the new oil. Therefore companies, organizations and hackers are always on the lookout for more and more data. This has increased the risk of hackers trying to mine important user data.

Risk Probability: 40%

Risk Impact:

Privacy violation may lead to accounts getting hacked, identity theft, impersonation, targeted ads as well as wrong people seeing the information. This could also harm the reputation of the platform and people would soon lose trust in the application. Information about properties could also be used by other competitors. Contact information about users may be used for marketing purposes.

This can be mitigated by outsourcing cloud security to cloud provider such as Cloudfare.

Risk Exposure:

RE = 0.4 x Rs. 40,000 = Rs. 16,000/month.

Risk Information Sheet:

Risk ID: 4	Date: 03/10/2023	Probability: 40%	Impact: Critical
Description: In today’s world, data is the new oil. Therefore companies, organizations and hackers are always on the lookout for more and more data. This has increased the risk of hackers trying to mine important user data.			
Refinement/Context: Sub condition 1: Hackers may attempt to steal personal information of users such as email addresses and passwords. Sub condition 2: Activity log of the users can also be targeted with the intention to analyse this data and provide targeted ads to the user. This is a serious breach of privacy.			
Mitigation/Monitoring: 1. Creation of automatic backups of the database. 2. Monitoring should be in place to verify the security state of: a. DNS records b. SSL certificates c. Web server configuration d. Application updates e. User access f. File integrity			
Management: RE computed to be Rs. 16,000 per month.			
Current Status: Mitigation steps to be initiated.			
Originator: Rishab Mandal		Assigned: Arnav Malvia	