Journal of Engineering Sciences

Vol 11, Issue 5,May/2020
ISSN NO:0377-9254

IT RISK MANAGEMENT

SYED SAIFUDDIN[1], R.CHIRANJEEVI[2], Mohammed Fazil[3]

[1]MBA II YEAR Scholar, Sdbasha1996@gmail.com, Samskruti College of Engg&Tech
[2]MBA II YEAR Scholar, Charan.rayabarapu1995@gmail.com,Samskruti College of Engg&Tech
[3]MBA II YEAR Scholar,Mohdfoofoo@gmail.com, Samskruti College of Engg&Tech

ABSTRACT :-

More and more companies are concern about their IT risks nowadays, especially the companies relying on IS (Information System) in business. The objective of this thesis focused on what risk in the case company should be paid the most attention to. In short, the aim is to find out what the biggest threat was in the case company and the reason. Moreover, when exploring the answer, it was possible to understand the process of managing IT risks.

The general methodology of this study is deductive research method. It aimed to check if the general IT risks found in literature in the case company. Moreover, the researcher was to develop the theory that organized cyber criminals and hackers are the riskiest security problem in business. Interviews and observation were carried out collect the data.

The study revealed that, inadequate anti-virus software protection is the biggest threat for the case company, and because the manager decided to ignore the existing problems, it will be an even bigger threat in the future.

Key words: IT risks, risk management, software protection.

INTRODUCTION:-

In the past decades, it was always heard from the press that crises are happening, such as the economic crisis, energy crisis and nuclear crisis. Those crises have an impact on individuals, businesses, organizations, even nations. It may result in incredible impacts if people ignore the upcoming risks. However, not all the people have the crisis awareness. People do
not care about it much until they have losses. The definition of risk 'Effect of uncertainty on objectives' (ISO 31000, 2009) was brought up. The bias of risk that represents badness has changed.

Hence, with a serious consideration, risk management is momentous. It is aimed to avoid the potential occurrence of risks, which is proactive. Indeed, not all probable threats are defined when people try to analyze the risks. There are still possibilities that the risk turns to be events that may cause negative impacts. Therefore, finding resolutions to redeem losses and reduce impacts, which refer to crisis management, is vital too (The difference between Crisis Management and Risk Management? 2010). Moreover, no matter which risks represent threats or opportunities, the impacts of event need to be assessed carefully.

As information technology is being used widely in companies to support their business, to secure IT becomes more significant. Every threat can be a disaster, even related to the organization's survival, especially for those companies that depend on the information systems. The better knowing of risks, the more secure the companies are. Therefore, managing IT risks in a company is vital to prevent from threats leading to disasters and to give countermeasures for better problem solving.

Statement of the problem :-

DTI (DTI Information Security Breaches Survey, 2006) reported that only less than 20 percent of small companies could survive without IT systems. In other words, large corporations operate their business with IT systems and the numbers has continued growing. Once the system breaks down or has something wrong, it may cause lots of direct losses, such as loss of system facilities, production, sales, communication, and control, also the business possibly fails. For instance, Comair, which is a huge airline company, valued to be $780 million, experienced a fatal hit due to the failure of crew-scheduling system. Thousands of passengers were affected by the crushed system. (Westerman & Hunter, 2007) Moreover, indirect consequences of IS disaster such as undetected fraud, financial loss through lack of billing and payment processing facilities, liability for payment of fines, damages and

compensation, loss of customers, diminished public standing. Indeed, any potential risks of information systems could turn out to be a disaster and cause loss.

Research objective :-

With the growing awareness for information technology security, it is worth to study IT risk management in an organization. Managing IT risks was carried out in case of business aiming at finding out which IT risk threatens the business most. Proactive perspectives would be reminded to have about potential risks for companies. In the case any loss is caused, this research would give some suggestions to do the remediation in a short time. It would also support improved decisions making for businesses and could protect them in a suitable way.

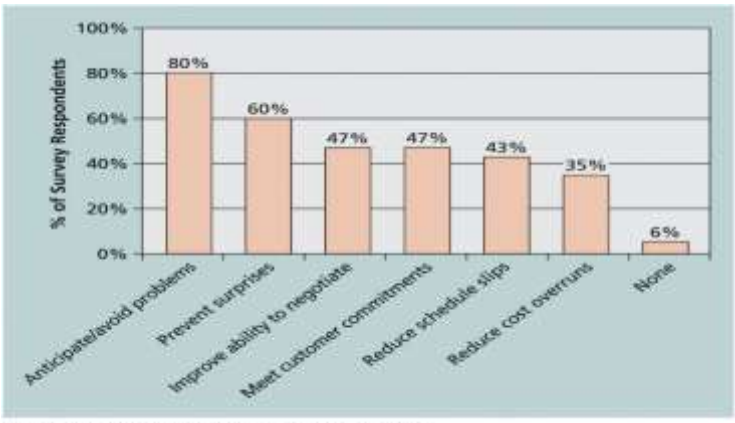
The company doing business in patent and intellectual property relies on IT systems. The researcher did her internship in this business and wanted to study the IT threats there for these purposes. Also, the research could help the company to be aware of its IT security. Therefore, the case is provided as an example of management of IT risks for better understanding.

OBJECTIVES:-

- Explain the concept of risk as it relates to project management, and list the advantages of managing project risks according to best practices
- Discuss the elements of planning risk management and the contents of a risk management plan
- List common sources of risks on information technology (IT) projects
- Describe the process of identifying risks and create a risk register and risk report
- Discuss qualitative risk analysis and explain how to calculate risk factors, create probability/impact matrixes, and apply the Top Ten Risk Item Tracking technique to rank risks
- Explain quantitative risk analysis and how to apply decision trees, simulation, and sensitivity analysis to quantify risks
- Provide examples of using different risk response planning strategies to address both negative and positive risks
- Discuss how to monitor risks
- Describe how software can assist in project risk management
- Discuss considerations for agile/adaptive environments

The Importance of Project Risk Management :-

- Project risk management is the art and science of identifying, analyzing, and responding to risk throughout the life of a project and in the best interests of meeting project objectives
- Risk management is often overlooked in projects, but it can help improve project success by helping select good projects, determining project scope, and developing realistic estimates
- Research shows a need to improve project risk management
- Study by Ibbs and Kwak shows risk management has the lowest maturity rating of all knowledge areas
- A similar survey was completed with software development companies in Mauritius, South Africa, and risk management also had the lowest maturity
- KLCI study shows the benefits of following good software risk management practices



Source: Kulik and Weber, KLCI Research Group

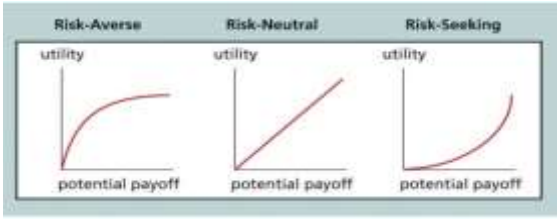
Figr of Benefits from Software Risk Management prctices

Global Issues :-

- Many people around the world suffered from financial losses as various financial markets dropped in the fall of 2008, even after the $700 billion bailout bill was passed by the U.S. Congress
- According to a global survey of 316 financial services executives, over 70 percent of respondents believed that the losses stemming from the credit crisis were largely due to failures to address risk management issues
- Worldwide banking and insurance sectors will spend about $78.6 billion on risk
- Information technologies and services in 2015, growing to $96.3 billion by 2018

The Importance of Project Risk Management :-

- A dictionary definition of risk is "the possibility of loss or injury"
- General definition of a project risk: an uncertainty that can have a negative or positive effect on meeting project objectives
- Managing negative risks involves a number of possible actions that project managers can take to avoid, lessen, change, or accept the potential effects of risks on their projects
- Positive risk management is like investing in opportunities
- Risk utility is the amount of satisfaction or pleasure received from a potential payoff
- Utility rises at a decreasing rate for people who are risk-averse
- Those who are risk-seeking have a higher tolerance for risk and their satisfaction increases when more payoff is at stake
- Risk-neutral approach achieves a balance between risk and payoff
- Project risk management processes
- Planning risk management: deciding how to approach and plan the risk management activities for the project
- Identifying risks: determining which risks are likely to affect a project and documenting the characteristics of each
- Performing qualitative risk analysis: prioritizing risks based on their probability and impact of occurrence
- Performing quantitative risk analysis: numerically estimating the effects of risks on project objectives
- Planning risk responses: taking steps to enhance opportunities and reduce threats to meeting



project objectives

- Implementing risk responses: implementing the risk response plans
- Monitoring risk: monitoring identified and residual risks, identifying new risks, carrying out risk response plans, and evaluating the effectiveness of risk strategies throughout the life of the project.

Planning Risk Management :-

- Main output of this process is a risk management plan
- Documents the procedures for managing risk throughout a project
- The project team should review project documents as well as corporate risk management policies, risk categories, lessons-learned reports from past projects, and templates for creating a risk management plan
- It is also important to review the risk tolerances of various stakeholders

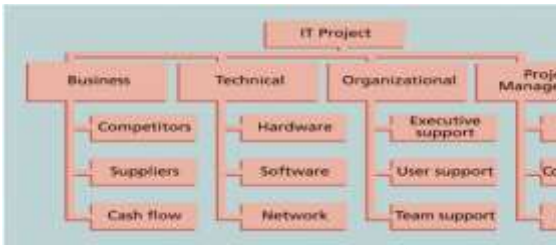
Additional plans:-

- Contingency plans: predefined actions that the project team will take if an identified risk event occurs
- Fallback plans: developed for risks that have a high impact on meeting project objectives, and are put into effect if attempts to reduce the risk are not effective
- Contingency reserves or allowances: funds included in the cost baseline that can be used to mitigate cost or schedule overruns if known risks occur

- Management reserves: funds held for unknown risks that are used for management control purposes

Common Sources of Risk on IT Projects :-

- Several studies show that IT projects share some common sources of risk
- The Standish Group developed an IT success potential scoring sheet based on potential risks
- Other broad categories of risk help identify potential risks
    1. Market risk
    2. Financial risk
    3. Technology risk
    4. People risk
    5. Structure/process risk
- A risk breakdown structure is a hierarchy of potential risk categories for a project



FIGR OF Common Sources of Risk on IT Projects

Identifying Risks :-

- Understanding what potential events might hurt or enhance a particular project
- You cannot manage risks if you do not identify them first
- Another consideration is the likelihood of advanced discovery
- Often viewed at a program level rather than a project level
- Suggestions for identifying risks: tools and techniques
    1. Brainstorming
    2. The Delphi Technique
    3. Interviewing
    4. SWOT analysis

Brainstorming:-

- Group attempts to generate ideas or find a solution for a specific problem by amassing ideas spontaneously and without judgment
- An experienced facilitator should run the brainstorming session
- Be careful not to overuse or misuse brainstorming
- Psychology literature shows that individuals produce a greater number of ideas working alone than they do through brainstorming in small, face-to-face groups
- Group effects often inhibit idea generation

Interviewing :-

- Fact-finding technique for collecting information in face-to-face, phone, e-mail, or virtual discussions
- Interviewing people with similar project experience is an important tool for identifying potential risks

SWOT analysis :-

- Strengths, weaknesses, opportunities, and threats
- Helps identify the broad negative and positive risks that apply to a project.

The Risk Register:-

- Important output of the risk identification process
- List of identified risks and other information needed to begin creating a risk register
- Contains the results of various risk management processes and that is often displayed in a table or spreadsheet format
- Tool for documenting potential risk events and related information
- Risk events refer to specific, uncertain events that may occur to the detriment or enhancement of the project

Risk register contents :-

1. Identification number for each risk event
2. Rank for each risk event
3. Name of each risk event

4. Description of each risk event
5. Category under which each risk event falls
6. Root cause of each risk
7. Triggers for each risk; indicators or symptoms of actual risk events
8. Potential responses to each risk
9. Risk owner or person who will own or take responsibility for each risk
10. Probability and impact of each risk occurring
11. Status of each risk

No.	Rank	Risk	Description	Category	Root Cause	Triggers	Potential Responses	Risk Owner	Probability	Impact
R44	1									
R21	2									
R7	3									

Risk report contents: -

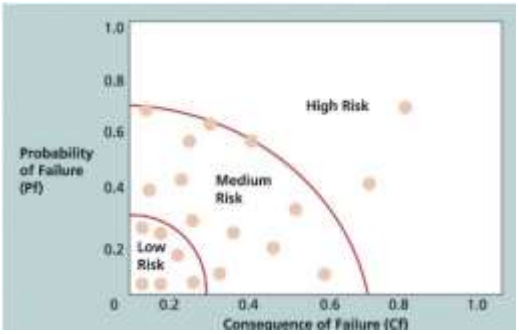
1. Sources of overall project risk
2. Important drivers of overall project risk exposure
3. Summary information on risk events

Performing Qualitative Risk Analysis:-

- Assess the likelihood and impact of identified risks to determine their magnitude and priority
- Risk quantification tools and techniques
    1. Probability/impact matrixes
    2. The Top Ten Risk Item Tracking
    3. Expert judgment

Using Probability/Impact Matrixes to Calculate Risk Factors:-

- Lists relative probability of a risk occurring on one side of a matrix or axis on a chart and the relative impact of the risk occurring
- List the risks and then label each one as high, medium, or low in terms of its probability of occurrence and its impact if it did occur
- Calculates risk factors
- Numbers that represent the overall risk of specific events based on their probability of occurring and the consequences to the project if they do occur.



FIGR OF Using Probability/Impact Matrixes to Calculate Risk Factors

Performing Quantitative Risk Analysis:-

- Often follows qualitative risk analysis, but both can be done together
- Large, complex projects involving leading edge technologies often require extensive quantitative risk analysis
- Main techniques
    1. Decision tree analysis
    2. Simulation
    3. Sensitivity analysis

Decision Trees and Expected Monetary Value (EMV):-

- A decision tree is a diagramming analysis technique used to help select the best course of action in situations in which future outcomes are uncertain
- Estimated monetary value (EMV) is the product of a risk event probability and the risk event's monetary value
- You can draw a decision tree to help find the EMV

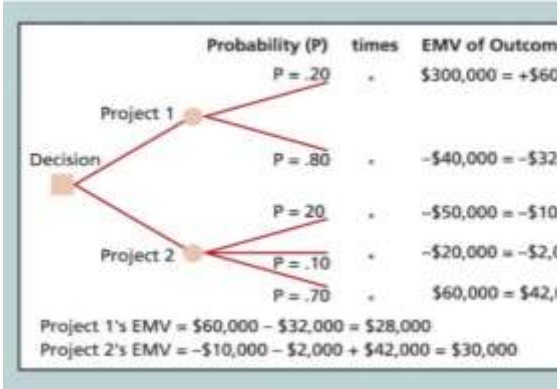


FIGURE OF Decision Trees and Expected Monetary Value.

Sensitivity Analysis:-

- Used to show the effects of changing one or more variables on an outcome
- For example, many people use it to determine what the monthly payments for a loan will be given different interest rates or periods of the loan
- Spreadsheet software, such as Microsoft Excel, is a common tool for performing sensitivity analysis

Simple test Sensitivity Analysis for determining break-even point.

Planning Risk Responses:-

- After identifying and quantifying risks, the organization must decide how to respond to them
- Basic response strategies for negative risks:-
    1. Risk avoidance
    2. Risk acceptance
    3. Risk transference
    4. Risk mitigation
    5. Risk escalation
- Basic response strategies for positive risks:-
    1. Risk exploitation
    2. Risk sharing
    3. Risk enhancement
    4. Risk acceptance
    5. Risk escalation

Technical Risks	Cost Risks	Schedule Risks
Emphasize team support and avoid stand-alone project structure	Increase the frequency of project monitoring	Increase the frequency of project monitoring
Increase project manager authority	Use WBS and CPM	Use WBS and CPM
Improve problem handling and communication	Improve communication, understanding of project goals, and team support	Select the most experienced project manager
Increase the frequency of project monitoring	Increase project manager authority	
Use WBS and CPM		

Figure of Planning Risk Responses

- It's also important to identify residual and secondary risks
- Residual risks: risks that remain after all of the response strategies have been implemented
- Secondary risks: direct result of implementing a risk response.

Implementing Risk Responses:-

- Main executing process performed as part of project risk management is implementing risk responses
- Key outputs :-
    1. Change requests
    2. Project documents updates

Monitoring Risks:-

- Involves ensuring the appropriate risk responses are performed, tracking identified risks, identifying and analyzing new risk, and evaluating effectiveness of risk management throughout the entire project
- Project risk management does not stop with the initial risk analysis
- Carrying out individual risk management plans involves monitoring risks based on defined milestones and making decisions

regarding risks and their response strategies

- Project teams sometimes use workarounds—unplanned responses to risk events—when they do not have contingency plans in place

Using Software to Assist in Project Risk Management:-

- Risk registers can be created in a simple Microsoft Word or Excel file or as part of a sophisticated database
- More sophisticated risk management software, such as Monte Carlo simulation tools, help develop models and use simulations to analyze and respond to various risks.

Risk countermeasures :-

Organizations give countermeasures in response to the identified threats to mitigate or prevent damages to business and the company. Countermeasures to physical security aim at protecting people from a harmful situation, IT assets from theft or damage. It also protects against unauthorized access to equipment, IT installations, electronic media and documentation.and furthermore, countermeasures should be given to dealing with sabotage or espionage.
It should prepare from three phases towards to the identified threat: which resolution to prevent or reduce the occurrence before it happens, when it is happening after it causes damages. When planning measures for physical threats, it can be divided into several steps (Philpott & Einstein, 2011):

- Deferrence:- Such as policies, procedures, technical devices and controls to protect people and IT assets.
- Detection:- Monitoring for potential breakdowns in protective mechanisms.
- Delay:- Delay getting enough time until security team comes to deal with it.
- Response:- Procedures and actions for responding to a breach
- Recovery:- Plan to continue business and operations like before the incident
- Reassessment:- Revisit the strategic plan to ensure the implementation right for the incident.

Physical security controls include exterior, entrance, administration, property and environment. Businesses are convincing enough for burglars to make the theft in the company. To secure office premises for keeping out thieves, damages, attacks, the company may use self-closing doors, window locks, security curtains or window, shutters or alarms. In case the building catches fire, fire detection and extinguisher systems have to be inspected often that they are working. The electric power needs emergency power failure controls, voltage maintenance, surge protection and back-up power in case of the power failure. Furthermore, the humidity control which makes power on needs to be ensured at a normal level.

Internal assets, especially for the server, have to be locked and kept eyes on it. The otiose extensions should unplug. It is better keeping the important paper information in the locker and shredding it before throwing out. The policy to warn employees not putting the sensitive documents on the table when they are not working on them could make. Moreover, employees should be encouraged to pick up the documents from printers, faxes, and photocopiers promptly. CCTV cameras could monitor visitors in case they walk to the sensitive areas.

Unauthorized disclosure:-
mainly reflected in

- Exposure of sensitive data
- Interception of sensitive data in transit

- Inference of sensitive data analysis
- Intrusion from system breach

Deception:- main features like

- An unauthorized entity masquerading as an authorized entity
- Falsification of data to deceive an authorized entity o repudiation

Disruption:- performances in

- Incapacitation of system operation
- Modification of the system function or data
- Hindering delivery of services through system operation

Usurpation:-mainly in

- Misappropriation of system resources
- Misuse leading to perform wrong function to system

Unauthorized disclosure may occur when users get access to the system through password, PIN code, or dynamic biometrics. Another possibility is when users get access to hardware with problems, like memory device. Therefore, it has to stop unauthorized access to the password file, or install intrusion detection software. What is more, it is also feasible to use account lockout mechanisms and automatic workstation log out or encrypted network links. Besides, the company should offer training for employees and enforce policies with strong passwords rather than a general one.

Nevertheless, it is still probably hard to keep systems or hardware safe with the power authentication, such as key loggers. After sneaky people get access to information assets, systems have to determine whether they have the right to access a resource. Except reliable information, systems also control the access to the particular fields in a file or applications. More than one authorization is required. The administrators could choose the system permission right and its level of people. Alternatively, individuals have access to certain resources by setting roles individually. Firewalls are the most general way to prevent routing attacks, protect vulnerable systems from outside, also regarded as monitoring point.

Attackers intrude packets through an outside source IP address, the best way is to reject external packets with an inside source IP address. Different attacks with different resolution, only when they are discovered and found out the attack type, the countermeasures could work. Thus, it is important to install intrusion prevention systems. They can block traffic as a firewall by using IDS algorithms.

Not only attacks in non-physical threats, malicious software is another huge potential risk to pay attention to. Nowadays, it is even more various, the malware known as virus1, worm2, logic bomb3, Trojan horse4, backdoor5, mobile code6, auto-rooter7, spammer/flooder8, key loggers9, rootkit10, zombie aka bot11.

The common malware around organization exists during communication, in transferring information and archiving process. More and more companies are using email instead of paper to communicate with internal people and clients. It allows simple, auditable information with multiple parties and more convenient to transfer records.

However, the convenience may become adverse because it is same easy to spread viruses. Therefore, a well-publicized and sensible e-mail policy that all staff is aware of should be established in the business. The policies can consider the requirement for permission before transmission of documents or possible control of types of file transmitted. Organizations may monitor e-mail legally on its own system.

Removable storage is an excellent device for data leakage. The use of facilities such as Truecyrpt allows companies to ensure that all data on removable storage encrypted. It is also possible to manage the ability of users to copy files to flash disks.

Backing up and archiving play important roles in business security. The malware is easy to be injected through SQL injection in systems. Only safe input is allowed in the construction of a command. There is another important countermeasure to be noticed, companies must apply security patches and upgrades on time to protect the system

CONCLUSIONS:-

When developing the intranet system, whoever the IT people or project students are, carelessness is the most dangerous for system crash. Without clear disciplines for IT usage, making loss is about time. Employees in the company should be educated to strengthen their IT security awareness and teach them how to reduce the risks.

How people use information system is based on their benefits, convenience is the first thinking condition. People with IT risks awareness care more about the information disclosure. Lack of IT knowledge can become vulnerable for attackers. Risk consciousness is low in the company because business goes smoothly with information technology. Only when the risks turn to be an event and cause loss, the company starts to take action to decrease the loss. People think their surroundings are safe without an obvious sign of distress.

On the whole, the top management decision is the key of the IT security factors in the case company. In addition, insiders' behavior and their awareness can enhance or lessen the risks.

Owing to the case company relying on information system to survive, and its data is much more worth, weak anti-virus software protection might lead to the data breach and ruin the business. A lagging action taken by manager side will bring more troubles and loss to the company. People think it is perfectly safe because there is no loss having made since years by using this anti-virus software. Losses mean risks. The anti-software software had not installed until researcher left the company; even there were instructions and warnings. Ignoring the existing problems could threaten the case company.

From the researcher's opinion, inadequate anti-virus software protection is the biggest threat for the case company, and because the manager decided to ignore the existing problems, it will threaten more.

PUBLISHED REFERENCES:-

- Cadle, J., & Yeates, D. (1991). Project Management for Information Systems.
- Cannell, C. F., & Kahn, R. L. (1968). Interviewing.
- Cohen, L., Manion, L., & Morrison, K. (2007). Research Methods in Education.
- CR, K. (1985). Research Methodology-Methods and Techniques.
- Creswell, J. W. (2008). Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research.
- Denzin, N. K., & Lincoln, Y. S. (1994). Handbook of Qualitative Research.
- Edmonds, W. A., & Kennedy, T. D. (2013). An Applied Reference Guide to Research Designs.
- Ghauri, P., & Gronhaug, K. (1995). Research Method in Business Studies.
- Hopkin, P. (2010). Fundamentals of Risk Management.
- Oppenheim, A. (1992). Questionnaire Design, Interviewing and Attitude measurement.
- Philpott, D., & Einstein, S. (2011). The Integrated Physical Security Handbook.
- Priest, A., & Wood, K. (2012). IT Risk Analysis.