Assignment

Subject risk and disaster management

Submitted to:
Engr.yaseen

Submitted by:
Saeed Ullah
ID 14670

Question no#1

ANSWER

What Is a Hazard

A hazard in safety management is a condition that poses danger to your organization, and can lead to an accident, incident, or other mishap if not mitigates.

A hazard satisfies ALL of the following conditions:

- **Is a dangerous condition,** such as an object, situation, circumstance, that **poses an unacceptable level of danger**;
- **Occurs once** in the safety mishap lifecycle;
- **Can lead directly to risk occurrence** (i.e., safety mishap, accident, etc.) if not mitigated; and
- **Arise from hazard mechanisms**, such as initiating actions and hazardous sources.

Though it is sometimes confused as other things, such as below, a hazard is ***NOT***:

- Benign objects (birds, mountains, people), which are hazardous sources;
- Safety mishaps, which are another way of saying risk occurrences;
- Damages, which are a product of risk occurrence; and
- Dangerous actions, which are associated with initiating mechanisms.

The only disagreement may be on what constitutes a "dangerous" situation. We advise you seek guidance from your compliance authority on this point.

Two Types of Threats

There are two types of threats that are used differently in different contexts. They are:

- General threats: the amount danger in a given circumstance; and
- Specific threats: a specific object, situation, behavior, etc., that corresponds to a rising level of danger within a given context.

What Is a General Threat

One type of threat is a **general threat,** which refers to the amount of danger in a given circumstance. It is used in the context of "threat level," such as:

- “There is no inherent threat in operations right now”; or
- “Given our current ERP, how much threat does a fire emergency pose?”; or
- “Terrorism is a [specific] threat that poses great [general] threat to aviation.”

What Is a Specific Threat

A threat can also be a generic term for a specific danger, such as an object, situation, behavior, etc. A specific danger can be identified as:

- Contributing to rising danger – such as a hazardous source or contributing factor; or
- Representing actualized danger – such as a hazard occurrence.

Some examples are:

- “In spring time, migrating birds are a threat we have to mitigate”;
- “That moose is no threat because he cannot get over the perimeter fence”; or
- “We have no plan for a bomb threat in our ERP.”

Difference between Hazard and Threat

Sometimes, hazard and threat might be used interchangeably. Consider the example of a flock of birds flying close to an aircraft. This flock is both a hazard and a threat.

However, because the concept of a threat is vaguer than the concept of a hazard, a threat is not always a hazard. Consider the example of:

- migrating birds, which are a hazardous source but not an actual hazard, or
- fatigue, which is a contributing factor.

The takeaway here is that a hazard occurs (is “actualized”) when your operations interact with hazard sources. A threat is simply a generic way to describe danger, whether the danger has actualized or not.

Question no#2

ANSWER

Identifying risk sources provides a basis for systematically examining changing situations over time to uncover circumstances that affect the ability of the project to meet its objectives. Risk sources are both internal and external to the project. As the project progresses, additional sources of risk can be identified. Establishing categories for risks provides a mechanism for collecting and organizing risks as well as ensuring appropriate scrutiny and management attention to risks that can have serious consequences on meeting project objectives.

Example Work Products

1. Risk source lists (external and internal)
2. Risk categories list

Subpractices

1. Determine risk sources.

Risk sources are fundamental drivers that cause risks in a project or organization. There are many sources of risks, both internal and external to a project. Risk sources identify where risks can originate.

Typical internal and external risk sources include the following:

- Uncertain requirements
- Unprecedented efforts (i.e., estimates unavailable)
- Infeasible design
- Competing quality attribute requirements that affect solution selection and design
- Unavailable technology
- Unrealistic schedule estimates or allocation
- Inadequate staffing and skills
- Cost or funding issues
- Uncertain or inadequate subcontractor capability
- Uncertain or inadequate supplier capability
- Inadequate communication with actual or potential customers or with their representatives
- Disruptions to the continuity of operations
- Regulatory constraints (e.g. security, safety, environment)

Many of these sources of risk are accepted without adequately planning for them. Early identification of both internal and external sources of risk can lead to early

identification of risks. Risk mitigation plans can then be implemented early in the project to preclude occurrence of risks or reduce consequences of their occurrence.
2. Determine risk categories.

Risk categories are "bins" used for collecting and organizing risks. Identifying risk categories aids the future consolidation of activities in risk mitigation plans.
The following factors can be considered when determining risk categories:

- Phases of the project's lifecycle model (e.g., requirements, design, manufacturing, test and evaluation, delivery, disposal)
- Types of processes used
- Types of products used
- Project management risks (e.g., contract risks, budget risks, schedule risks, resource risks)
- Technical performance risks (e.g., quality attribute related risks, supportability risks)

A risk taxonomy can be used to provide a framework for determining risk sources and categories.

Risk base on source:

Below are few risk base on source that can be available in your project as well. They are:

Schedule: Whether you get the hardware or software out on time, just like planned.
Scope: It is always a risk; whether you have covered all the work required. It will cost you if you have missed any important requirement.

Resource: This is also an aspect that is unpredictable; you can't expect availability of resources as planned. The planned resources can be used for some other projects as well, in that case you need to get someone new thus creating a problem in both schedule and cost. Sometimes in quality also, in case of inexperience.

Quality: The deliverable can be of poor quality due to some other imposed factors, making it a huge risk.

Cost: Estimation of cost can be a risk in your project; if there is something you have planned to purchase and if it is not available, it can prove costly, as you have to wait for this particular item for a longer period.

Apart from above, sources of risk can be organized into categories such as customer risk, technical (product) risk, and delivery risk. Within each category, specific sources of risk can be identified and risk reduction techniques applied.
Material and equipment risks:

• Required hardware will not be delivered on time.
• Access to the development environment will be restricted.
• Equipment will fail.

Customer risks:

Customer risk is related to the customer's key success factors for the project. A project is not successful if the customer is not successful with the process. It can be sub-divided as follows:

• Customer resources will not be made available as required.
• Customer staff will not reach decisions in a timely manner.
• Deliverables will not be reviewed according to the schedule.
• Knowledgeable customer staff will be replaced with those less qualified.
• Conflict within the customer organization about the desirability or feasibility of the

Technological risks:

Technical risk arises from the capability of the technical solution to support the requirements of the customer. It can be categorized as follows as well:

• The technology will have technical or performance limitations that endanger the project.
• Technology components will not be easily integrated.
• The technology is unproved and will fail to meet customer and project requirements.
• The technology is new and poorly understood by the project team and will introduce delays.

Delivery Risks:

Delivery risk is related to the ability of the complete team to deliver against the plan at the cost and schedules estimated, like;

• System response time will not be adequate.
• System capacity requirements will exceed available capacity.
• The system will fail to meet functional requirements.

Unpredictable risks:

• The office will be damaged by fire, flood, or other methods.
• A computer virus will infect the development environment or operational system.

Project management risks:

• The inexperience of the project manager will result in budget or schedule slippages.
• Management will deem this project to have a lower priority for resources and attention.

Resource risks:

• Main staff may not be available.
• Key skill sets will not be available when needed.
• Key staff will be lost during the project.
• Subcontractors or vendors will below-perform and fail to meet the milestones.

QUESTION NO 3

ANSWER:

Introduction

Over the last few years, the public transport industry in many developing countries has been involved in a process of deep transformation. At present, personal mode usage is more than public transport mode, causes. series of problems in daily life like, traffic congestion, delay, air pollution, noise pollution and large amount of energy wastage which has a negative impact on environment as well as on public health. Mobility requirements in metropolitan cities causes continuous growth of personalized vehicles leading to pollution and traffic congestion. To reduce the current pollution level, congestion and make the cities environment friendly, it is necessary to encourage the commuters to use the public transport system. To provide the desired service delivery level for public transport, it is essential to evaluate the existing transport systems using a reliable performance evaluation technique which can eventually help in enhancing the transit service delivery to their trusted passengers.

Performance Evaluation

Performance evaluation of public transport system requires to understand the terms on behalf of performance of the system to be evaluated. The evaluation can be done in two ways i) based on present perception of users about the service deliverd ii) based on the feedback provided by experienced evaluation team. Performance evaluation is defined as the technique to evaluate how good or bad is the performance of a transit service is under the prevailing operating condition. The performance of transit system can be enumerated based on two distinct dimensions i.e., *Service* and *Service quality*. *Service* is described as "the business transaction that take place between a donor (Service provider) and Receiver (Customer) in order to produce an outcome that satisfies the customer" (Ramaswamy, 1996). Whereas, *Service quality* gives the measure of how well the service level delivered to the commuter's as per their expectation. Parasuraman (1988) and Gronroos, (1984) defines service quality as a comparison between customer expectation and perception of service

Factors Effecting Service Quality

Estimation of service quality in terms of user perception is purely based on psychological behavior of the commuters. It is necessary to understand the key parameters upon which transit performance depends, as these factors internally and externally affect the user perception and creates a perception of the transit system in the user's mind. The selection of factors differs from one public mode to another.

Various number of factors to define the service quality. The different service attribute dimensions are described in
Table 1.

Researcher's Name	**Type of Transit System**	**Service Quality Attributes**
Parasuraman et al.(1985)	Bus, Train, Metro	Reliability, Assurance, Tangibles, Empathy and Reliability
TRB USA (1999)	Buses, Tram, Metro and Rail	Reliability, Competence, Access, Courtesy, Communication, Credibility, Security, Understanding of customer and Tangibles.
Chang, Hepu and Yu-Hern (1999)	Bus transit system	Safety, Comfort, Convenience, Operation, Social duty (Vehicle air pollution level, Vehicle noise level)
Y. Tyrinopolus and Antoniou (2008)	Bus and Metro	Service frequency, Service hour, Time table info, Behavior of personnel , Distance and time to access and regress trip, Waiting condition at stop ,Driver behavior, Information in vehicle, Accessibility w.r.t Disabilities, Transfer distance, Transfer waiting time, Info regarding transfer
Margarita Friman (2009)	Buses	Frequency, Travel time, Punctuality, price, Information, Cleanliness, Bus comfort, Staff behavior, Seat availability, Bus stop security, Safety from accident, On board security, Bus stop condition and Info bus stop
Eboli and Mazzulla (2009)	Buses	Route characteristics, Service characteristics, Service reliability, Comfort, Cleanliness, Fare, Information, Safety and security, Personnel and Customer service
Sudin Bag and Som Sankar Sen (2012)	Metro	Air condition & lighting, Seating and free space, Inside atmosphere, Parking space, Smart card and multi ride facilities, Staff behavior, Management attitude, Helpfulness of staff, Attentiveness and resolve quarries,

Marta Rajo, Harnan, Luigi and Angel (2012)	Bus and Train transit system	Journey time, frequency, Condition of vehicle, Route , Number of intermediate stop, Bus stop location, Connection with other transport mode, Time table info, Possibility of buying ticket at home, Journey distance, Cost of journey, Number of delay bus and train services, Average speed of journey,
Adris.A.Putra (2013)	Bus Transit System	Safety, Accessibility, Affordable Tariff, Capacity, Regularity, Swift and fast, On time, Integration, Efficicent, Easyness, Orderly, Security, Cozy, Low Pollution,

Method of collecting user perception data

Surveys and interviews are the most popular methods of primary data collection. The User perception data can be collected by conducting a Station/Stop Survey or Workplace survey by direct face to face interview or by using alternative (telephonic interviews) indirect techniques. Paper-and-Pencil Interview (PAPI) is very popular for data collection, in which an enumerator asks questions to the respondent by holding a printed set of questions.

Performance Evaluation Models

Major works on "performance evaluation" began after 1970, many of the transportation planners and researchers had started trying different approaches and techniques for developing different models to estimate the transit system performance in terms of user perception. Since service quality is a qualitative parameter hence modeling of qualitative parameters creates more difficulties.

SERVQUAL Model

Parasuraman (1985) suggested a model for measuring service quality by measuring the gap between the service delivered and service received. It is mostly used by market researchers to identify customer satisfaction on behalf of service delivered. This model represents the service quality in terms of 10 dimensions namely, Reliability, Responsiveness, Competence, Access, Courtesy, Communication, Credibility, Security, understandability and Tangibles. But after 1988, these ten components were merged to formulate five distinct dimensions namely, Reliability, Assurance, Tangibles, Empathy, Responsiveness .These components are collectively called RATER. However, limitation of this model is SERVICE QUALITY (SERVQUAL) factors are inconsistent and it is not incomprehensible for different applications [9].

Impact Score Technique (IST)

Federal Administration of the U.S (1999) developed a simple and effective measurement method to evaluate customer satisfaction for transit services termed as Impact Score Technique. The IST approach determines the relative impact of attributes on user satisfaction by measuring relative decrease in user satisfaction when there is a problem with the attributes. For each attribute the whole sample is divided into two categories, user who faced a recent problem and those who haven't faced any problem (within past 30 days). The gap between mean overall ratings of two groups is known as "Gap Score". A composite index is found out by multiplying gap score to problem incident rate.

Important Performance Analysis (IPA)

IPA was first introduced by Martilla (1977) . IPA is also known as quadrant analysis which is used in many areas due to its ease of identification of different quality parameter that can lead to the improvement in Service quality.

QUESTION NO 4

ANSWER;

SECURITY VULNERABILITIES OF A UNIVERSITY CAMPUS:

- Students and others share user information. Campus visitors pop USB sticks into networked machines. Hackers find their way into an internal network through carelessly discarded information from an open screen or from an infected workstation.

campus security people up at night, and big challenges that schools should address to make themselves more resistant to cyber threats.

Phishing and Social Engineering Attacks

One of the biggest challenges with university cybersecurity is the sheer amount of hacking that goes on in these environments. Schools have to deal with a unique mix of user levels, including students who are often young, and relatively trusting, and are not employees of the organization — so they're less controlled.

For example, research shows a full 90% of malware attacks originate through e-mail. Various types of spoofing and spear-phishing campaigns entice students and others to click on illegitimate links that can usher in a Trojan Horse to do damage to a network system or compromise the security of information. Many of these kinds of phishing are cost, high — which leads to an inundation of hacker activity that schools have to keep in top of, by somehow segmenting network systems, by shutting down compromise parts of the system, or by some other high-tech means.

With this in mind, better security often starts with identifying separate pools of users — for example, administrative staff versus faculty and students, and then customizing controls and access for each of these groups individually.

The IT Crunch: Limited Resources

The challenge of limited resources and funding for university cybersecurity generally speaks for itself. The above kinds of network monitoring and cybersecurity engineering have significant costs attached to them, and many universities simply find it difficult allocate the manpower or the funding to address cybersecurity issues.

Regulatory Burdens and Secure Data Efforts

Another part of this challenging cybersecurity environment is that schools and universities have big compliance burdens under many different types of applicable regulation.

Some campus leaders tend to focus on items like NIST 800-171 and the use of controlled unclassified information, just because there is a deadline on for this particular type of compliance right now. However, regulations like

ERPA are also critical. Even HIPAA puts pressure on schools to tighten up cybersecurity, since as healthcare providers, schools may hold student health data. Third-party cloud providers often offer FEDRAMP certification and other qualifications for cybersecurity on their side of the fence — but that doesn't fully bring a university into compliance unless it can bring its own internal systems up to standards.

System Malware — Zero Day Vulnerabilities and More

Universities and colleges also must anticipate situations where hackers may exploit existing system vulnerabilities. They have to look at continuing support for operating systems and other technologies.

There is a reasonable expectation that manufacturers will make adequate security available, but this doesn't absolve the university of having to look for security loopholes and close them. This means evaluating architectures — for example, can hackers get host names, IP addresses and other information from devices like printers?

It also means using multi-factor authentication to control user activity. It means understanding how malware will enter a system, and anticipating attacks. The good news is that modern security tools go well beyond the perimeter of a network to seek out harmful activity if they are set up right and controlled and observed well, they can dramatically decrease risk.

Protecting Personally Identifiable Information

At the heart of many of these cybersecurity efforts is the daunting struggle to protect all sorts of personally identifiable information, from simple student identifiers to financial data and medical data, from grades to Social Security numbers and items that identity thieves might use. The above-mentioned regulations are part of the drive to secure this type of data, along with more general standards and best practices for enterprise. Simply put, data breaches cost money, both in damage control, and in the reputation of the school itself.

In some ways, this ongoing data vigilance is hard for schools, because the academic world isn't necessarily into strict control of information. But it's also hard in a practical sense, because so many cybersecurity architectures just can't handle modern challenges, like a WannaCry infiltration or other attacks that exploit common vulnerabilities. Many schools have up to a dozen or more security tools in place, but many of these tools don't talk to each other or share data well, and so they become less effective as a comprehensive protective force.

There are some things that schools can do to protect PII — one technique is to limit end-user storage and access — for instance, restricting the ability of students to simply move floods of information to the cloud, or navigate sensitive internal network areas freely.

Another strategy is to use internal monitoring tools to inspect network traffic for suspicious activity.

For example, peeking at the header and footer of data packets can show the origin of data transfers, unless there is spoofing or some sophisticated type of deception involved. Some schools will go further and fully decrypt data packets to see what's inside them. However, this practice can involve getting into the philosophy of privacy, where schools are wary of digging into network traffic because they see their monitoring as too intrusive to students or other users. In addition, emerging European privacy standards may put some pressure on schools in the U.S. and observation activities.

End-User Awareness and Training

Another way for schools to increase safety is for them to conduct vibrant types of end-user to limit decryption awareness campaigns.

This starts with educating end-users on how malware gets into a system — asking them not to click on suspicious e-mails or use inbound links, but instead to always do online banking and perform other transactions through a secure website.

Schools can also educate on the kinds of data that are most likely the targets of hacking activity — research data, student grades, health information or other sensitive data sets that hackers really want to get their hands on.

- On the other side of the equation, schools should also work on improving their internal security postures — figuring out how they will respond to attacks, and how they will preemptively safeguard systems against everything from phishing to ransomware.