SUBJECT: Risk and Disaster Management

Assignment#01 dated: 12/07/2020

Instructor: Engr. Yaseen Mahmood

Submitted by: Waqas Amin

ID No: 14817

M.S Construction Engineering Management

Department of Civil Engineering, INU Peshawar.

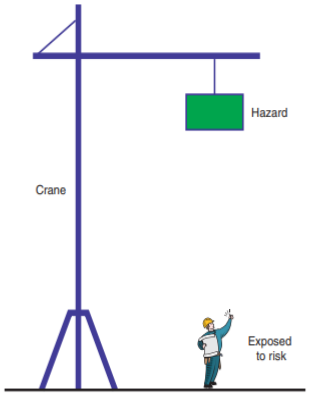
1. What is the difference between hazards and threats? Provide examples.

HAZARD: *A hazard is anything that has the potential to cause harm, ill health and injury, damage to property, products or the environment, production losses or increase liabilities. It pertains to the physical object, situation or setting which poses a threat to life, property or any other thing.*

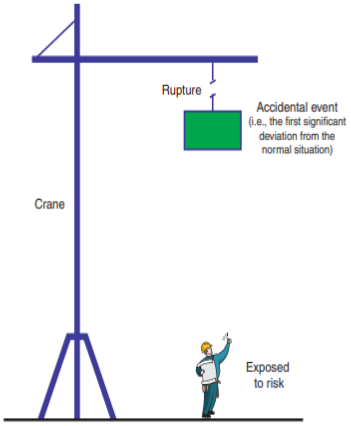
The six main categories of hazards are:

1. ***Biological Hazards:*** *Biological hazards include viruses, bacteria, insects, animals, etc., that can cause adverse health impacts. For example, mold, blood and other bodily fluids, harmful plants, sewage, dust and vermin.*
2. ***Chemical Hazards:*** *Chemical hazards are hazardous substances that can cause harm. These hazards can result in both health and physical impacts, such as skin irritation, respiratory system irritation, blindness, corrosion and explosions.*
3. ***Physical Hazards:*** *Physical hazards are environmental factors that can harm an employee without necessarily touching them, including heights, noise, radiation and pressure.*
4. ***Safety Hazards:*** *These are hazards that create unsafe working conditions. For example, exposed wires or a damaged carpet might result in a tripping hazard. These are sometimes included under the category of physical hazards.*
5. ***Ergonomic Hazards****: Ergonomic hazards are a result of physical factors that can result in musculoskeletal injuries. For example, a poor workstation setup in an office, poor posture and manual handling.*
6. ***Psychosocial Hazards:*** *Psychosocial hazards include those that can have an adverse effect on an employee's mental health or wellbeing. For example, sexual harassment, victimization, stress and workplace violence*

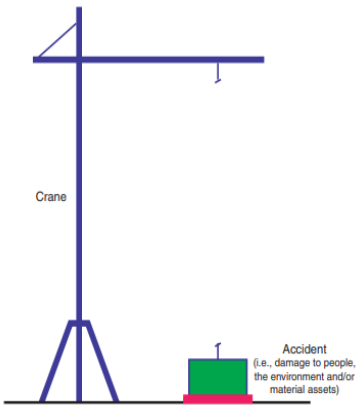
Hazard



Hazardous event



Accident



Threat: *Threat is defined as a possible cause that will release the hazard to become a top event (The accident which occurs as e result of the hazard being released).*

For example:

High voltage is a threat, it may release the hazard of electric cable to become top event i.e electric shock

High temperature is a threat, it may release the hazard of volatile fluid on site to become top event i.e may explode.

Similarly incompetent person working on a high rise scaffolding is threat, there is a possibility of falling from the height.

Other examples of threat are Corrosion, Overpressure, erosion, Radiation, environmental conditions.

2. Define risk and provide a classification of risk based on its sources. Provide an example for each risk source.

RISK*: The term 'risk' is used to mean the chance of gaining or losing something worthy such as health, wealth, name, environment, etc. It is the probability of occurrence of an undesirable or adverse event, although not necessarily so, caused by a particular activity of inactivity. Therefore, the risk is the result of the probability of an event and its outcomes.*

In finer terms, risk is the likelihood of quantifiable loss, damage, injury, liability or any other negative outcome, resulting from internal or external exposure, which can be mitigated through preventive action. It is originated from different situations and can be of various types:

- *Dynamic Risk: Also known as speculative risk, it is a situation wherein there is a possibility of either profit or loss.*
- *Static Risk: A situation in which the probability of profit is nil, and there is the only possibility of loss or no loss, is called as pure risk or static risk.*
- *Fundamental Risk: The type of risk which affects a large group of people or the economy as a whole, such as natural calamities or inflation.*
- *Particular Risk: The risk that adversely affects individuals not the whole economy, e.g. accident, theft, etc.*
- *Subjective Risk: Subjective risk refers to the risk that depends on an individual's mental state at a particular time.*

- *Objective Risk: The relative difference of actual loss from the anticipated loss is called objective risk.*
- *Financial Risk: The risk whose result can be measured in monetary terms*
- *Non-financial Risk: it is one, whose measurement in monetary terms is not possible.*

Examples:

1. *Working alone away from your office can be a hazard. The risk of personal danger may be high.*
2. *Electric cabling is a hazard. If it has snagged on a sharp object, the exposed wiring places it in a 'high-risk' category.*
3. *Water is a hazard, jumping into water without knowing how to swim is a risk.*
4. *Gasoline is a hazard, lighting a match near gasoline may cause top event of explosion putting it on a high risk.*
5. *Similarly excavating a trench with excavator is a hazard, texting during the excavation may places it in a risk of damaging values property or workers working round about.*

3. How would you assess the performance of a transportation system of a city?

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.

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. PAPI surveys should be carried out by taking proper precaution by randomly selecting a person from the population, so that it eliminate the chance of nonresponsive and responsive biasness. At present

internet based survey methods have taken over the place of PAPI method as it reduces the manpower, time and provide readymade scrutinized results. However, a major drawback of this method is its inability to cover of the population who are not familiar with the internet.

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. The impact score is obtained from this it listed in the descending order to identify top attributes that drives major satisfaction. This technique is one of the simple methods for the estimation of important attributes which can impact the satisfaction of the user and it would be easily understood by the operator as well. The limitation of this technique is that all the data have to be collected within the past 30 days

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. In IPA, user satisfaction is translated into Cartesian diagram where two lines perpendicularly

divide it into four sections as shown in Figure 1. Where (Q) represents the average of average scores of level of implementation of all factors and (P) represents the average of average scores of the importance of all factors.

Conclusion:

Among above discussed models, SERVQUAL model is one of the simplest model to enumerate the service quality but it isn't vastly used in transportation reasearch domain as it fails to specify a proper model and its attributes are inconsistent. The IPA and CSI based models provide good results but are unable to give the reasons for the impact of each attributes on service quality, while Artificial Neural Network (ANN) and Fuzzy inference based methods presents better accuracy in analysis of service quality attributes, obvious drawback of ANN and fuzzy logic stems from the fact that it fails to yield any direct numerical model as an output. If one makes comparison on all the available models, it can be inferred that the Structure Equation Modeling (SEM) is one of the best modelling approach in the field of research on service quality measurement.

4. Define security vulnerabilities of a university campus

Vulnerability: The propensity or predisposition to be adversely affected. Vulnerability encompasses a variety of concepts and elements including sensitivity or susceptibility to harm and lack of capacity to cope and adapt.

Vulnerability refers to the characteristics and circumstances of a community, system or asset that make it susceptible to the damaging effects of a hazard.

There are many aspects of vulnerability, arising from various physical, social, economic, and environmental factors. Examples may include poor design and construction of buildings, inadequate protection of assets, lack of public information and awareness, limited official recognition of risks and preparedness measures, and disregard for wise environmental management. Vulnerability varies significantly within a community and over time

Vulnerability with at least one known, working attack vector is classified as an exploitable vulnerability. The window of vulnerability is the time from when the vulnerability was introduced to when it is patched.

Security vulnerabilities of a university campus:

Classification of Vulnerability:

Vulnerabilities are classified according to the asset class they are related to:

- *hardware*
  - *susceptibility to humidity*
  - *susceptibility to dust*
  - *susceptibility to soiling*
  - *susceptibility to unprotected storage*
- *software*
  - *insufficient testing*
  - *lack of audit trail*
  - *design flaw*
- *network*
  - *unprotected communication lines*
  - *insecure network architecture*
- *personnel*
  - *inadequate recruiting process*

    - *inadequate security awareness*
- *physical site*
    - *area subject to flood*
    - *unreliable power source*
- *organizational*
    - *lack of regular audits*
    - *lack of continuity plans*
    - *lack of security*

Causes of Vulnerability:

- *Complexity: Complex systems increase the probability of a flaw, misconfiguration or unintended access.*
- *Familiarity: Common code, software, operating systems and hardware increase the probability that an attacker can find or has information about known vulnerabilities.*
- *Connectivity: The more connected a device is the higher the chance of vulnerability.*
- *Poor password management: Weak passwords can be broken with brute force and reusing passwords can result in one data breach becoming many.*
- *Operating system flaws: Like any software, operating systems can have flaws. Operating systems that are insecure by default and give all users full access can allow viruses and malware to execute commands.*
- *Internet usage: The Internet is full of spyware and adware that can be installed automatically on computers.*
- *Software bugs: Programmers can accidentally or deliberately leave an exploitable bug in software.*
- *Unchecked user input: If your website or software assume all input is safe it may execute unintended SQL commands.*
- *People: The biggest vulnerability in any organization is the human at the end of the system. Social engineering is the biggest threat to the majority of organizations.*

SECURITY VULNERABILITIES OF A UNIVERSITY CAMPUS:

<u>Phishing and Social Engineering Attacks</u>

One of the biggest challenges with university cyber security 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 cyber security generally speaks for itself. The above kinds of network monitoring and cyber security engineering have significant costs attached to them, and many universities simply find it difficult allocate the manpower or the funding to address cyber security issues.

Regulatory Burdens and Secure Data Efforts

Another part of this challenging cyber security 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 FERPA are also critical. Even HIPAA puts pressure on schools to tighten up cyber security, since as healthcare providers, schools may hold student health data. Third-party cloud providers often offer FEDRAMP certification and other qualifications for cyber security 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 have to 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 cyber security 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 cyber security 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*