Name: SHEHARYAR KHAN

ID no. 13544

Final term Assignment

Subject: RISK AND DISASTER MANAGEMENT

July 12, 2020

Question no : 1

What is the difference between hazards and threats? Provide examples

Hazard: A source of danger that may cause harm to an asset.

A hazard is:

- A property, a situation, or a state.
- Not an event but a prerequisite for the occurrence of a hazardous event..
- Often, but not always, related to energy of some kind.

- Acoustic
- Atmospheric
- Chemical
- Corrosive
- Electrical
- Electromagnetic
- Explosive, pyrophoric
- Flammable
- Gravitational
- Hydraulic
- Kinetic (linear)
- Kinetic (rotational)
- Magnetic
- Mechanical
- Nuclear
- Pathogenic
- Pneumatic
- Potential
- Pressure
- Thermal
- Toxic

Triggering event:

- An event or condition that is required for a hazard to give rise to an accident.
- Triggering events and hazardous events may be the same.
- Triggering events may also be interpreted as events that cause a hazardous event.
- Active failures: Events that trigger unwanted events.
- Latent conditions: Not triggers, but conditions that may increase the probability of active failures.

Classification of hazardous:

Natural hazards:

- Floods, earthquakes, tornados, tsunamis, lightning

Technological Hazards:

- Industrial facilities, structures, transportation systems, consumer products, pesticides, pharmaceuticals

Organizational hazards:

- Long working hours, inadequate competence

Social hazards:

- Assault, war, sabotage, communicable disease

Specific hazardous:

- Drug abuse, alcohol, smoking, and so on
- Types of technological hazards
- Mechanical, electrical, radiation
- What are the effects (type of harm)?
  - Cancer, suffocation, pollution, burn
- Where is the origin of the hazard?
  - Endogenous – “inside” the system
  - Exogenous – “outside” the system

Mechanical hazards

- Kinetic energy
- Acceleration or retardation
- Sharp edges/points
- Potential energy
- High pressure
- Vacuum
- Moving parts
- Rotating equipment
- Reciprocating equipment
- Stability/toppling problems
- Degradation of materials

Dangerous materials

- Explosive
- Oxidizing
- Flammable
- Toxic
- Corrosive
- Carcinogenic
- Electrical hazards
- Electromagnetic
- Electrostatic
- Short circuit

- Overload
- Thermal radiation

Threat:

- Anything that might exploit vulnerability.
- Any potential cause of an incident can be considered a threat
- Closely related to hazard
- A threat is a hazard, but a hazard need not be a threat

Threat agent:

- A person, organization, thing, or entity that acts, or has the power to act, to cause, carry, transmit, or support a threat.
- Who could want to exploit vulnerabilities, and how they might use them against the system
  - Intention, capacity, and opportunity
- **Availability:**
  - The accessibility of systems, programs, services, and information when needed and without undue delay
- **Confidentiality:**
  - The sensitivity of information or assets to unauthorized disclosure, recorded as classification or designation, each of which implies a degree of 'loss' should unauthorized disclosure occur
- **Integrity:**
  - The accuracy and completeness of information and assets and the authencity of transactions
- **Compromise:**
  - Unauthorized disclosure, destruction, removal, modification or interruption.

Technical failure:

- Vulnerability:
  - A weakness of an asset or group of assets that can be exploited by one or more threat agents, for example, to gain access to the asset and subsequent destruction, modification, theft, and so on, of the asset or parts of the asset.
  - The weaknesses may be physical, technical, operational, and organizational.
- **Failure:**
  - The termination of the ability of an idea to perform a required function.
  - In other words: A failure is the non-fulfillment of a functional (or performance) requirement.

Failure mode:

- Consider a water pump:
- A required function of the pump is to "pump water.
- The functional requirement related to this function is that the output of water should be between 100 and 110 liters of water per minute.
- The pump has failed if the output of water is outside this interval.

  Failure mode:
  The effect by which a failure is observed on a failed item.

General failure:

- A failure mode is a state and specifies the actual deviation from the performance requirements of the item.
- This definition is not totally clear, but a failure mode should tell us in which way an item is no longer able to fulfill a required function.
  - Failure during operation
  - Failure to operate at a prescribed time
  - Failure to cease operation at a prescribed time
  - Premature (spurious) operation

Example:

- Fail to open (on demand) I Fail to close (on demand)
- Cannot fully close
- Leakage through (dripping)
- Leakage out (from tap seals)
- Too high temperature
- Too low temperature

Failure mechanism:

- A physical, chemical, or other process that leads to failure.

Examples of failure mechanisms include

- Corrosion
- Erosion, Fatigue, Primary failure:
  Caused by natural aging that occurs under conditions within the design envelope of the item.
- Secondary failure:
  Caused by excessive stresses outside the design envelope of the item.
- Command fault:
  A failure caused by an improper control signal or noise (sometime referred to as a transient failure).
- Critical:
  A failure that causes immediate and complete loss of the system's capability of providing its output.
- Degraded:
  A failure that is not critical but that prevents the system from providing its output within specifications.
- Incipient:
  A failure that does not immediately cause loss of a system's capability of providing its output, but which, if not attended to, could result in a critical or degraded failure in the near future.

Question 4) Define security vulnerabilities of a university campus?

SECURITY VULNERABILITIES OF A UNIVERSITY CAMPUS:

Sometimes it seems like the security challenges facing American colleges and
Universities are never-ending. 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. Here are six of the things that keep 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 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 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 FERPA 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

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 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, peaking 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. to limit decryption 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 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 ransom ware.

Security Vulnerability of university campus Examples

A Security Vulnerability is a weakness, flaw, or error found within a security system that has the potential to be leveraged by a threat agent in order to compromise a secure network.

There are a number of Security Vulnerabilities, but some common examples are:

Broken Authentication: When authentication credentials are compromised, user sessions and identities can be hijacked by malicious actors to pose as the original user.

SQL Injection: As one of the most prevalent security vulnerabilities, SQL injections attempt to gain access to database content via malicious code injection. A successful SQL injection can allow attackers to steal sensitive data, spoof identities, and participate in a collection of other harmful activities.such as sarkhad university data was blocked by indian engineer.

Cross-Site Scripting: Much like an SQL Injection, a Cross-site scripting (XSS) attack also injects malicious code into a website. However, a Cross-site scripting attack targets website users, rather than the actual website itself, which puts sensitive user information at risk of theft.

Cross-Site Request Forgery: A Cross-Site Request Forgery (CSRF) attack aims to trick an authenticated user into performing an action that they do not intend to do. This, paired with social engineering, can deceive users into accidentally providing a malicious actor with personal data.

A. Computer vulnerabilities Sample university network is given in Fig. 1, It is a fact now that computer vulnerabilities are steadily increasing since 1995 . Malicious activities are still rising despite all the efforts to reduce it which includes:

- More patches and updates supplied by vendors
- Increased Public awareness and media attentions.
- Creating computer crime units.
- More tools in the security arsenal.
- The creation of Computer Crime and Intellectual Property Section by The Department of Justice

B. Base Profile Metrics Once discovered and analyzed, there are certain aspects of vulnerability that remain unchanged, assuming the initial information is complete and exact. The properties of the vulnerability will remain unchanged overtime and will not change by changing the environment. The access and impact qualities are captured by the base profile metrics. The following are the metrics used to identify if the vulnerable system is exploitable. These are of following types:

- Access Vector- identify wither the vulnerability can be exploited locally or remotely.
- Access Complexity- it measures the attack complexity in order to exploit a given vulnerability once the attacker access the system.
- Authentication- identify wither authentication is required or not to exploit the vulnerability.
- Confidentiality Impact- this metric will measure the impact of confidentiality in the exploited system
- Integrity Impact- it measure how much the integrity have been impacted on the exploited system.
- Availability Impact- in an exploited system how much the availability has been impacted.

Question 2:

Definition:

- Risk implies future uncertainty about deviation from expected earnings or expected outcome. Risk measures the uncertainty that an investor is willing to take to realize a gain from an investment.
  - Risks are of different types and originate from different situations.
  - We have liquidity risk, sovereign risk, insurance risk, business risk, default risk, etc.
  - Various risks originate due to the uncertainty arising out of various factors that influence an investment or a situation.

Systematic Risk :

- **Market Risk :**
  - Market Risk is the risk that the value of an investment will decrease due to movements in market factors. The reason for such uncertainty is market forces represent. in two markets, viz Bull Market and Bear Market
- **Interest Rate Risk :**
  - Interest rate risk is the possibility of an unexpected. change in interest rates prevailing in the market. which affects the value of an investment adversely. Generally the value of debt instruments like bonds. debentures, commercial papers. etc. is directly affect. by Interest Rate Risk.
- **Purchasing Power Risk :**
  - Purchasing power risk is the possible reduction in the purchasing power of the expect. returns. Due the high rate of inflation. there is erosion in the purchasing power of money, which results in decrease in the returns.

Unsystematic Risk:

- Unsystematic risk may be specification to an industry or company and is caused due to deficiencies in one or more of the following
  - Lack of managerial ability
  - Technological advancement in the process of production.
  - Procurement of raw materials
  - Lack of human resources
  - **Change in consumer preference**

Business Risk:

- Market business risk is a part of the unsystematic risk.
- Which basically comes from the operational activities of the business?
- Due to certain inbuilt deficiencies in the operations of the business.
- Due to certain inbuilt deficiencies in the operations of a company.

Internal Business Risk :

Internal risk is related to with the operational effectiveness of a company. The operational effectiveness of a company is measured in terms of the level of its targeted achievements and keeping the promises made to its investors.

1. Research and Development (R&D)
2. fixed Cost
3. Single Product
4. Sales variation
5. Personal management

External Business Risk :

External business risks are the risk caused by the circumstances. which are external to a company's business. The company has no control over these circumstances or factors.

1) Social and Regulatory Factors: e.g. Telecommunication. Similarly the profitability of banks is affected by some of the regulatory directions issued on the lending policies.
2) Political risk : Frequent changes in the Govt and its policies have a negative impact on business environment.
3) Business cycle :boom and recession is the best example business cycle. Textile industry will be in boom for short period after that the demand will be decrease.

Financial Risk :

- Financial risk is a function of financial leverage which is the use of debt in the capital structure.
- The presence of debt in the capital structure creates fixed payments in the form of interest which is a compulsory payment to be made whether the company makes profit or loss.
- This fixed interest payment creates more variability in the earnings per share(EPS) available to equity share holders.
    - Credit Risk
    - Currency Risk
    - Country Risk
    - Economic Risk
    - Liquidity Risk

Measurement Risk :

- Risk in investment is associated with return.
- The risk of an investment cannot be measured without reference to return.
- The return. in turn. depends on the cash inflows to be received from the investment to return.
- The return in turn depends on the cash inflows to be received from the investment.
- Let us consider the purchase of a share.
- While purchasing an equity share. an investor expects to receive future dividends declared by the company.
- In addition he expects to receive the selling price when the share is finally sold.

Example:

Suppose a share is currently selling at Rs.120. An investor who is interest in the share anticipates that the company will pay a dividend of Rs. 5 in the next year. Moreover he expects to sell the share at Rs. 175 after one year. The expected return from this can Ix calculated as follows.

Expected Return

The expected return of the investment is the probability weighted average of all the possible returns. If the possible return are denoted by Xi and the related probabilities are p(Xi). the expected return may be represented as

Key information to Reminder before

Possible returns = would indicate the expected return from the investment. (denoted by Xi) Probability of Occurrence = This indicates the risk of the investment.(denoted by p(Xi))

Example

A share is currently selling at Rs.50. It is expected that a dividend of Rs.2 pershare would be paid during the year and the share could be sold at Rs. 54 at the end of the year. Calculate the expected return from the share.

Solution : R = Forecast Dividend + Forecasted end of the period stock - 1

Initial Investment

Example (based on Previous example)

Calculate expected return

Possible Returns (In %) X_i	Probability of Occurrence $p(X_i)$
30	0.10
40	0.30
50	0.40
60	0.10
70	0.10

Calculation of Expected Return

Possible Returns (In %) X_i	Probability of Occurrence $p(X_i)$	$X_i\ p(X_i)$
30	0.10	3
40	0.30	12
50	0.40	20
60	0.10	6
70	0.10	7
Here, the expected return is 48%		48

Risk

Expected returns are insufficient for decision-making. The risk aspect should also be considered. The most popular measure of risk is the variance or standard deviation of the probability distribution of possible returns.

Example:

Calculate the expected return and the standard deviation of returns for a stock having the following Probability distribution of returns

Possible Returns (In Per Cent) X_i	Probability of occurrence $p(X_i)$
-24	0.05
-10	0.15
0	0.15
12	0.20
18	0.20
22	0.15
30	0.10

Example:

A stock costing Rs. 250 pays no dividends. The possible prices that the stock might sell fax at the end of the year and the probability of each are

Possible Prices (Rs.)	Probability of occurrence $p(X_i)$
200	0.10
230	0.25
250	0.35
280	0.20
310	0.10

:

A) What is the expected return?

B) What is the Standard Deviation of the returns?

6 Mr. RKV invested in equity shares of Wipro limited, it's anticipated returns and associated probabilities are given below:

Return %	Probability
-15	0.05
-10	0.10
5	0.15
10	0.25
15	0.30
20	0.10
30	0.05

You are required to calculate:

(a) The expected rate of return.

(b) Risk in terms of SD.

Question No 3: How would you assess the performance of a transportation system of a city?

Answer:

Performance Evaluation:

To fulfill the high demand for better public transport system, there is a need to establish attractive, safe and highly sophisticated public transport systems. In this regard, it is essential to conduct a thorough evaluation of public transport modes. This paper gives an overview and presents the possible ways to identify and measure the performance of public transit system. It presents the definition and literature in respect of different measurement models towards the public transit performance assessment coupled with comparative study of different measurement models that can be used for performance evaluation.

The Asia-Pacific region has witnessed rapid population growth and urbanization. In 2016, half of the world's 4 billion urban dwellers lived in the region, and today 19 of the world's 31 megacities are in the region. According to recent projections, by 2030 urban population in the region will reach 2.7 billion (56 per cent of total population), and by 2050 this number will reach 3.2 billion (63 per cent urban share)

The provision of sustainable urban transport is becoming a major issue due to rapid urbanization worldwide, including in the Asia-Pacific region.

The performance of a transportation system is affected by several factors such as human factors, vehicle factors, acceleration characteristics, braking performance etc. These factors greatly influence the geometric design as well as design of control facilities. Variant nature of the driver, vehicle, and roadway characteristics should be given importance for the smooth, safe, and efficient performance of traffic in the road.

Transportation system in a city performs depends both on public investment and policy, and on millions of decisions made daily by consumer-travelers about whether, where, how and when to travel. Understanding how people make travel choices is key to understanding urban transportation problems and potential solutions.

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 based on present perception of users about the service delivered based on the feedback provided by experienced evaluation team. Performance evaluation is defined as the technique to evaluate how well 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 Whereas, Service quality gives the measure of how well the service level delivered to the commuter’s as per their expectation.

Performance Evaluation Models:

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.

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.

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.

Customer Satisfaction Index (CSI)

Customer Satisfaction Index is a method to determine the level of satisfaction that has been achieved with respect to the service delivered. CSI was proposed by Supranto (1997). CSI can be computed by using the average value of the level of expectation and the performance of each service item.

Ordered Legit Model:

The ordered logic models are regression models for ordinal dependent variables and the genesis behind using this model is to understand how well that output can be predicted by the responses to other questions.

Structural Equation Modeling (SEM):

Structural Equation Modeling (SEM) methodology is a powerful multivariate analysis technique in which a set of relationships between observed and unobserved variables are established. It is relatively new method which began in the 1970s (Fornell, 1981), it has been widely applied in various domain of research, including psychology, education, social science, economics, statistics, etc.

Soft Computing Techniques:

At present soft computing techniques are also being used by researchers for performance appraisal of different transit system. Among different soft computing techniques Artificial Neural Network (ANN), Fuzzy logic and Genetic algorithm now a day’s quite popular.