ASSISGNMENT # 01

RISK AND DESASTER MANAGEMENT

Submitted By: ENG: FAIZA SANA

Roll Number: 14662

Question No.1. What is the difference between hazard & Threats? Provide Examples.

ANSWER No.1.

HAZARD: A hazard is defined as "a dangerous phenomenon, substance, human activity or condition that may cause loss of life, injury or other health impacts, property damage, loss of livelihoods and services, social and economic disruption, or environmental damage"

OR

A rare or extreme natural or human made event that threatens to adversely affect human life ,property or activity to extent of causing the disaster.

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

THREAT: a statement of an intention to inflict pain, injury, damage, or other hostile action on someone in retribution for something done or not done.

Types of Hazards	Types of Threats
Natural Hazards: Are naturally occurring physical phenomena caused either by rapid or slow onset events e.g. earth quake, flood, extreme temperature	General threats: the amount danger in a given circumstance
Man-Made Hazards: They are caused by some human interaction; whether human induced intentionally or caused simply from an accident from something we built. Industrial accidents, Terrorism or other criminal acts	Specific threats: a specific object, situation, behavior, etc., that corresponds to a rising level of danger within a given context

Examples:

HAZARDS

THREATS

Question No.2. Define RISK and provide a classification of risk based on its sources. Provide an example for each risk source

ANSWER No.2.

Risk is measure of expected losses due to hazard events of particular magnitude occurring in a given area over a specific time period. Level of risk depends upon Nature of hazard, Vulnerability of affected element, Economic value of affected element.

Risks are of 3 types Business Risks, Non Business Risks, Financial Risks

1. **Business Risks:** These types of risks are taken by business enterprises themselves in order to maximize shareholder value and profits. As for example, Companies undertake high-cost risks in marketing to launch a new product in order to gain higher sales.

2. **Non Business Risks:** These types of risks are not under the control of firms. Risks that arise out of political and economic imbalances can be termed as non-

business risk.

3. **Financial Risk**: Financial Risk as the term suggests is the risk that involves financial loss to firms. Financial risk generally arises due to instability and losses in the financial market caused by movements in stock prices, currencies, interest rates and more.

Examples Business Risks	Examples Non Business Risks	Examples Financial Risk
Financial risk: Taking on a loan to secure a new phase of development means betting on higher profits that will allow paying down the line of credit on a fixed timeline.	The **risk** of wider economic changes affecting the rate of interest on long-term sources of finance, Model Risk, Operational Risk (fraud, misconduct, failure of internal controls or audit systems, natural disasters), Settlement risk, Accounting risk (changes in GAAP/IFRS and comparability issues, managed earnings, etc.).	**Liquidity risk: C**omes in two flavors for investors to fear. The first involves securities and assets that cannot be purchased or sold quickly enough to cut losses in a volatile market. Known as market liquidity risk this is a situation where there are few buyers but many sellers. The second risk is funding or cash flow liquidity risk. Funding liquidity risk is the possibility that a corporation will not have the capital to pay its debt, forcing it to default, and harming stakeholders.
Strategic risks: Are those that arise from the fundamental decisions that directors take concerning an organization's objectives. Essentially, strategic risks are the risks of failing to achieve these business objectives	Regulatory risk, Legal risk (counterparty does not honor a contract) Tax risk, Sovereign risk (if you are trading EM debt for example) & Political risk, Performance, netting risk, Key Man risk, Political risk	**Speculative risk:** Is one where a profit or gain has an uncertain chance of success. Perhaps the investor did not conduct proper research before investing, reached too far for gains, or invested too large of a portion of their net worth into a

		single investment.

Question No.3. How would you assess the performance of a transport system of a city?

ANSWER No.3.

The measurement of transit performance represents a very useful tool for ensuring continuous increase of the quality of the delivered transit services, and for allocating resources among competing transit agencies. Transit service quality can be evaluated by subjective measures based on passengers' perceptions, and objective measures represented by disaggregate performance measures expressed as numerical values, which must be compared with fixed standards or past performances. Transportation system is a source of considerable environmental damage affecting a wide range of receptors, including human health, flora and fauna, and the built environment. The main environmental effects concern air pollution, climate change, noise, impacts on nature and landscape, soil and water deterioration; other effects include, as an example, visual intrusion in cities.

Mobility demand of people living in urban and metropolitan areas is continuously growing because of the desire to participate in increasingly varied activities motivated by physiological, psychological and economic needs. Interdependencies among activities entail complex travel choices involving the generation of trip-chains and travel patterns. In order to satisfy this ever-changing mobility demand, people tend to use individual motorized transport modes. Performance measurement can be defined as the assessment of an organization's output as a product of the management of its internal resources (money, people,vehicles, facilities) and the environment in which operates. Performance measurement is very useful for different aims: assisting in evaluating the transit system's overall performance, assessing management performance expectations of the transit system in relation to community objectives, assessing management performance and diagnosing problems such as disproportionate cost in relation to service, allocating resources among competing transit properties, providing a management control system for monitoring and improving transit services, facilitating the accountability sought by government funding agencies and demanded by legislators, regional and transit authority boards, and the general public. Performance in general terms refers to any evaluation or comparison measure.

A performance measure can be considered as a quantitative or qualitative characterization of performance. Each of these measures has certain indicators that are used to signify transit performance for each particular measure. A performance indicator is more specifically a performance measure used to document progress toward a performance goal, and to monitor performance. A review of the literature on transit performance reveals that not all agencies use the same terms for performance measures.

In addition, views of performance-based allocation and how indicators are calculated vary tremendously. Therefore, in the literature, there are various classifications of the transit performance measures, some are more schematic, and others more articulate.

Question No.4. Define security vulnerabilities of a university campus?

ANSWER No.4.

Sometimes it seems like the security challenges facing 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 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 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 — 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 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. 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 ransomware.

THE END