IQRA NATIONAL UNIVERSITY OF IT AND EMERGING SCIENCES PESHAWAR

SUBJECT NAME: RISK AND DISASTER MANAGEMENMT

TOPIC NAME: ASSIGNMENT

DATE: 12 JULY 2020

SUBMITTED TO: ENGR. YASEEN MEHMOOD

SUBMITTED BY: SHAHID RASHID

CLASS ID: 15287

DEPARTMENT OF CONSTRUCTION ENGINEERING MANAGEMENT

Q1. What is the difference between hazards and threats? Provide examples:

Ans:

HAZARDS:

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.

THREATS:

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

A threat refers to a new or newly discovered incident that has the potential to harm a system or your company overall. There are three main types of threats:

- **Natural threats**, such as floods, hurricanes, or tornadoes
- **Unintentional threats**, like an employee mistakenly accessing the wrong information
- **Intentional threats**, such as spyware, malware, adware companies, or the actions of a disgruntled employee

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.

Q2. Define risk and provide a classification of risk based on its sources. Provide an example for each risk source:

Ans:

RISK:

“Risk is defined in financial terms as the chance that an outcome or investment's actual gains will differ from an expected outcome or return”.

Risk includes the possibility of losing some or all of an original investment. Quantifiably, risk is usually assessed by considering historical behaviors and outcomes. In finance, standard deviation is a common metric associated with risk. Standard deviation provides a measure of the volatility of asset prices in comparison to their historical averages in a given time frame.

Classification of Risk Based on its 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.

Provide an Example for each Risk Source:

1. **Purpose and Need not well-defined**: The first project risk example is the risk related to the need and purpose of the project. This is a medium type of risk but it can get transferred to the high project risk category if the project is impacted by this factor.

2. **Incomplete project design and deliverable definition:** The second project risk example is incomplete project design and deliverable definition. It is a low-risk factor but can eventually turn out to be a high-risk factor if not controlled beforehand.

3. **Difficulty in defining and understanding project schedule**: Every project must have a specific time period to be completed. If there is no set schedule or if there is difficulty in understanding the project schedule then this project risk example will arise. It is included in the low-risk category but can turn out to cause a medium risk to the project.

4. **Risks related to budget:** There may be times when the costs go beyond the revenue and in such scenarios, this project risk example arises. There may be uncertainty in every business activity related to the future and when the cost exceeds revenue, the risk factor becomes severe.

5. **Resistance to changes:** This is another project risk example in which if a project does not implement changes with the changing trends, it will cause issues in the project. For example, if technology has to be changed in an organization, and the team members resist the changes, it will cause a problem with respect to the working of the project.

6. **Risks related to the resources:** The next project risk example is related to the resources. This risk arises if the project is not able to acquire the relevant resources, for example, skilled workers, finances, and so on.

7. **Lack of control over staff priorities:** The next project risk example is related to the staff members. If a project fails to create a backup for team members, then the project will be delayed which is indeed a negative aspect that may give rise to other risk factors.

8. **Risk factors related to disputes:** A project is handled by many people and it is likely to happen that disputes can arise due to different thoughts, different, and different expectations. So, therefore, this is included in the project risk examples.

9. **Unplanned work risk:** There are a number of tasks to be performed by each one related to the project. When tasks are not planned efficiently then this type of risk arises and the project will have cases of delayed work more than the tasks which are being completed.

10. **Communication issues:** One of the other project risk examples includes the communication channel between the people related to the project. Due to lack of communication, there will be no clarity, and instead, confusion will arise which will be stressful for the efficient running of the project.

11. **Risk related to errors:** Another project risk example is related to the errors. The team members must not be forced to complete tasks in a limited time period as this will increase the

possibility of getting errors. This type of project risk also arises when the team is working under pressure.

12. **Escalating project conflicts not reported timely:** This gives rise to another project risk examples. According to this, conflicts arising in the team and outside the team are not handled timely due to which the conflicts arise. This is a low to medium risk factor if it causes an impact on the project.

13. **Delay in projects:** Delay in competing for earlier project causes this risk to occur in the current project.

Q3. How would you assess the performance of a transportation system of a city?

Ans: Assess the Performance of a Transportation System of a City

The provision of sustainable urban transport is becoming a major issue due to rapid urbanization worldwide, including in the Asia-Pacific region. The adoption of the 2030 Agenda for Sustainable Development, with its. Sustainable Development Goals, adds new impetus to efforts to address global development challenges, including urban transport. Sustainable Development Goal target focuses on improving accessibility for all, with an emphasis on public transport. Measuring the state of urban transport and evaluating urban transport policies and their implementation can support assessments of urban transport contributions to sustainable development. Increasingly, selected urban transport indicators and indices are useful for the assessment of urban transport systems and services and also reflect the state of urban transport performance among cities. There is, however, no established system of indicators and

indices to measure, monitor and report on sustainable transport for cites in the Asia-Pacific region. Within the urban transport theme included in the Regional Action Programmed for Sustainable Transport Connectivity in Asia and the Pacific, phase I (2017–2021), a study on the assessment of urban transport systems was envisaged. A collaborative research study was embarked on in 2016 to identify key urban transport indicators that could constitute an index to measure the sustainability of urban transport systems and policies in the Asia-Pacific

context. The concept of a sustainable urban transport index was presented at the Expert Group Meeting on Planning and Assessment of Urban Transportation Systems, held in Kathmandu in

September 2016. The Meeting supported the concept and provided feedback on identifying indicators and developing an index. The Regional Meeting on Sustainable Urban Transport Index, held in Jakarta in March 2017, finalized the index and recommended that the Committee of Transport, at its fifth session, in 2018, consider endorsing the sustainable urban transport index for its regional application in Asian cities.

Q4. Define security vulnerabilities of a university campus.
Ans:

Vulnerability:

A vulnerability refers to a known weakness of an asset (resource) that can be exploited by one or more attackers. In other words, it is a known issue that allows an attack to succeed. For example, when a team member resigns and you forget to disable their access to external accounts, change logins, or remove their names from company credit cards, this leaves your business open to both intentional and unintentional threats. However, most vulnerabilities are exploited by automated attackers and not a human typing on the other side of the network.

Testing for vulnerabilities is critical to ensuring the continued security of your systems. By identifying weak points, you can develop a strategy for quick response. Here are some questions to ask when determining your security vulnerabilities:

- Is your data backed up and stored in a secure off-site location?
- Is your data stored in the cloud? If yes, how exactly is it being protected from cloud vulnerabilities?
- What kind of network security do you have to determine who can access, modify, or delete information from within your organization?
- What kind of antivirus protection is in use? Are the licenses current? Is it running as often as needed?
- Do you have a data recovery plan in the event of a vulnerability being exploited?

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 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 abovementioned 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.