Enhancing Digital Government and Economy

Cyber Security Course

Classwork-12

Submitted by,

Name: Koushiki Devi Agarwalla

Batch: JUR2B11

ID: 2111271

Phases of Risk Analysis

- Asset identification
- Vulnerability identification
- Threat Assessment
- Probability Quantification
- Impact Analysis
- Countermeasures determination

The following outlines various types of threats, commonly referred to as risk types:

Environmental Threats

Environmental threats arise from the natural surroundings or geographical location of your business. These threats encompass events such as floods, tsunamis, earthquakes, volcanic eruptions, tornadoes, blizzards, lightning storms, and hurricanes.

Human-Made Threats

Human-made threats, also known as manmade threats, result from human actions, whether deliberate or accidental. Examples of these threats include computer viruses, fires, theft, vandalism, and acts of sabotage.

Internal and External Threats

It's essential to recognize that threats can be classified as either internal or external. **Internal threats** originate from individuals within the organization, such as a disgruntled employee deliberately deleting customer data or an employee accidentally removing a critical file. Protecting against both types of threats is crucial. **External threats**, on

the other hand, come from outside the organization, exemplified by cybercriminals attempting to breach your mail server or website.

Common vulnerabilities that may exist:

- **No system hardening**
- **No physical security**
- **No security controls on data**
- **No administrative controls**

The following is a list of common examples of threats:

- **Theft**
- **System hacked from inside**
- **System hacked from outside**
- **Natural disasters**
- **Hardware failures**
- **Fraud**

The formula **Risk = Probability × Loss** provides a clear and quantitative approach to understanding and managing risks. By evaluating both the likelihood of risk events and their potential consequences, organizations can make informed decisions to enhance their overall risk management strategies.

Application of the Formula

Calculation: By multiplying the probability of a risk event by the potential loss, organizations can calculate a numerical value representing the overall risk. For example, if the probability of a data breach is 20% (0.2) and the estimated loss from that breach is $100,000, the risk value

would be: Risk=0.2×100,000=20,000\text{Risk} = 0.2 \times 100,000 = 20,000Risk=0.2×100,000=20,000

Decision-Making: This calculation assists organizations in prioritizing risks based on their potential impact, allowing them to allocate resources effectively for risk mitigation strategies. Higher risk values may require more immediate attention or comprehensive controls, while lower values may be monitored with less urgency.