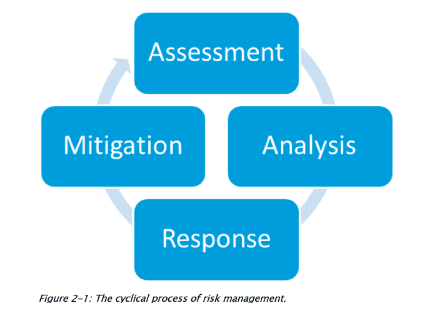
**Analyzing Risk**

Risk Management:

In the information world risk comes in many different forms. If a risk is not managed properly, it could result in discloser, modification or interruption of a critical asset. Risk management is a cyclical process that includes four phase:



**Some common used terms**

Asset: A resource that your organization needs to function

Vulnerability: A weakness in the configuration of hardware or software

Threat: An event that can cause harm to the asset

Threat vector: A tool, or mechanism, the hacker uses to exploit a weakness on a system

Threat actor :The person (hacker) using the threat vector to compromise the system

Threat target : The system or device being attacked

Risk : When the threat to an asset can cause harm to the organization—typicallyM resulting in a financial loss

Risk analysis: The identification and planning of mitigation techniques to reduce and manage the risks to your organization

**IDENTIFYING ASSESTS**

The first phase of performing a risk analysis, also known as a risk

assessment, is to identify the assets within the organization and the

value of those assets. This phase is also known as asset identification.

For example, if a company earns revenue by selling products online,

the web server hosting the e-commerce web site would be considered

an asset to the company. During this phase, be sure to focus on identifying the assets instead of worrying about things like the threats to those assets—that will come in the next phase.

**Risk Assessment Process**

IDENTIFYING THREAT OF EACH ASSEST(THREAT ASSESSMENT)

Once you have identified the assets in the organization, you then turn your focus to threat assessment, which involves identifying the threats to each of the assets identified in the first phase.

Continuing with the preceding example, a company e-commerce web site has a number of potential threats; for example, the system could be hacked via a buffer overflow exploit or an SQL injection attack.

The web server could also experience a hard drive failure, which could cause the system to be down for a long time, resulting in lost revenue.

When performing the threat assessment, it is important to identify threats from different sources—or different types of disasters.

There are environmental threats, person-made threats, and both internal and external threats.

THREAT ASSESSMENT

The following identifies these different types of threats, also referred to as risk types:

Environmental An environmental threat results from the environment, or location, in which your business operates.

Environmental threats include, among others, floods, tsunamis, earthquakes, volcanic eruptions, tornados, blizzards, lightning storms, and hurricanes.

Person-made A person-made threat, also known as a manmade threat, is a threat that does not exist naturally but instead is a result of human actions, whether intentional or unintentional.

Examples of manmade threats would be viruses, fire, theft, vandalism, and sabotage. Internal and external It is important to note that threats can be either internal or external. An internal threat comes from someone inside the organization. This could be a threat such as a disgruntled employee intentionally deleting customer data, or an employee accidentally deleting a file. You need to protect from both types of threats. An external threat comes from outside the organization and could be, for example, someone on the Internet trying to hack into your mail server or your web site.