What is Risk Analysis

Risk analysis is the process of identifying and analysing potential issues that could negatively impact key business initiatives or projects. This process is done in order to help organizations avoid or mitigate those risks.

Performing a risk analysis includes considering the possibility of adverse events caused by either natural processes, like severe storms, earthquakes or floods, or adverse events caused by malicious or inadvertent human activities. An important part of risk analysis is identifying the potential for harm from these events, as well as the likelihood that they will occur.

Enterprises and other organizations use risk analysis to:

- anticipate and reduce the effect of harmful results from adverse events;
- evaluate whether the potential risks of a project are balanced by its benefits to aid in the decision process when evaluating whether to move forward with the project;
- plan responses for technology or equipment failure or loss from adverse events, both natural and human-caused; and
- identify the impact of and prepare for changes in the enterprise environment, including the likelihood of new competitors entering the market or changes to government regulatory policy.

Benefits of risk analysis

Organizations must understand the risks associated with the use of their information systems to effectively and efficiently protect their information assets.

Risk analysis can help an organization improve its security in a number of ways. Depending on the type and extent of the risk analysis, organizations can use the results to help:

- identify, rate and compare the overall impact of risks to the organization, in terms of both financial and organizational impacts;
- identify gaps in security and determine the next steps to eliminate the weaknesses and strengthen security;
- enhance communication and decision-making processes as they relate to information security;
- improve security policies and procedures and develop cost-effective methods for implementing these information security policies and procedures;
- put security controls in place to mitigate the most important risks;
- increase employee awareness about security measures and risks by highlighting best practices during the risk analysis process; and
- understand the financial impacts of potential security risks.

Done well, risk analysis is an important tool for managing costs associated with risks, as well as for aiding an organization's decision-making process.

Steps in risk analysis process

The risk analysis process usually follows these basic steps:

1. **Conduct a** risk assessment **survey:** This first step, getting input from management and department heads, is critical to the risk assessment process. The risk assessment survey is a way to begin documenting specific risks or threats within each department.

2. **Identify the risks:** The reason for performing risk assessment is to evaluate an IT system or other aspect of the organization and then ask: What are the risks to the software, hardware, data and IT employees? What are the possible adverse events that could occur, such as human error, fire, flooding or earthquakes? What is the potential that the integrity of the system will be compromised or that it won't be available?
3. **Analyze the risks:** Once the risks are identified, the risk analysis process should determine the likelihood that each risk will occur, as well as the consequences linked to each risk and how they might affect the objectives of a project.
4. **Develop a** risk management **plan:** Based on an analysis of which assets are valuable and which threats will probably affect those assets negatively, the risk analysis should produce control recommendations that can be used to mitigate, transfer, accept or avoid the risk.
5. **Implement the risk management plan:** The ultimate goal of risk assessment is to implement measures to remove or reduce the risks. Starting with the highest-priority risk, resolve or at least mitigate each risk so it's no longer a threat.
6. **Monitor the risks:** The ongoing process of identifying, treating and managing risks should be an important part of any risk analysis process.

The focus of the analysis, as well as the format of the results, will vary depending on the type of risk analysis being carried out.

Qualitative vs. quantitative risk analysis

The two main approaches to risk analysis are qualitative and quantitative. Qualitative risk analysis typically means assessing the likelihood that a risk will occur based on subjective qualities and the impact it could have on an organization using predefined ranking scales. The impact of risks is often categorized into three levels: low, medium or high. The probability that a risk will occur can also be expressed the same way or categorized as the likelihood it will occur, ranging from 0% to 100%.

Quantitative risk analysis, on the other hand, attempts to assign a specific financial amount to adverse events, representing the potential cost to an organization if that event actually occurs, as well as the likelihood that the event will occur in a given year. In other words, if the anticipated cost of a significant cyberattack is $10 million and the likelihood of the attack occurring during the current year is 10%, the cost of that risk would be $1 million for the current year.

A qualitative risk analysis produces subjective results because it gathers data from participants in the risk analysis process based on their perceptions of the probability of a risk and the risk's likely consequences. Categorizing risks in this way helps organizations and/or project teams decide which risks can be considered low priority and which have to be actively managed to reduce the effect on the enterprise or the project.

A quantitative risk analysis, in contrast, examines the overall risk of a project and generally is conducted after a qualitative risk analysis. The quantitative risk analysis numerically analyses the probability of each risk and its consequences.

The goal of a quantitative risk analysis is to associate a specific financial amount to each risk that has been identified, representing the potential cost to an organization if that risk actually occurs. So, an organization that has done a quantitative risk analysis and is then hit with a data breach should be able to easily determine the financial impact of the incident on its operations.

A quantitative risk analysis provides an organization with more objective information and data than the qualitative analysis process, thus aiding in its value to the decision-making process.