

Risk Management

Dealing with risks through risk management is the most fundamental basis for rational decision-making in security, yet it is inadequately addressed in almost all of the products on the market and services offered today.

Risk refers to the uncertainty that surrounds future events and outcomes. It is the expression of the likelihood and impact of an event with the potential to influence the achievement of objectives.

In its most basic formulation, risk management can be reasonably defined as:

Risk management is a systematic approach to taking informed courses of action under uncertainty by understanding risk-related issues and integrating that understanding into the decision-making process.

In order to effectively manage risks, it is incumbent on organizations of all sizes and sorts to rationalize systematic decision-making processes. This then implies the application of metrics and optimization at some level. Many vendors supply simplistic calculators to allow multiplication of a likelihood or event realization rate by an expected average loss to generate an expected loss, and some vendors even supply limited capabilities for characterizing select lists of events in various approaches, but no product today or in the foreseeable future has the capacity to do the hard work necessary to substantially facilitate a process that can take business issues effectively into account to make sound business decisions. The fundamental item that is lacking in today's technology in this regard is the technology of modeling and simulation.

Modeling is the art of creating representations of systems that abstract out the irrelevant while including enough information about the relevant to meaningfully characterize features of interest.

In the case of risk management for an organization, the models must serve to represent the organization in context by including relevant factors and relationships with sufficient granularity and clarity to allow meaningful distinctions to be drawn without perfect information, excessive volume of data, or difficulty in collecting necessary data.

Simulation is a method that allows models to be repeatedly exercised under varying assumptions and deviations to yield reasonably anticipatory results.

In the risk management context, simulation is applied to models under varying conditions stipulated by the systematic approach to risk management in order to understand the implications of different strategies for courses of action on the achievement of objectives.

Today, most enterprises lack the knowledge, will, or resources to implement effective risk management approaches, and vendors do not provide the means to accomplish this with the tools they provide. The only solution available is the use of outside vendors on a consulting basis to help provide knowledge, support the creation of internal will, and help develop the internal resources necessary to support effective risk management.