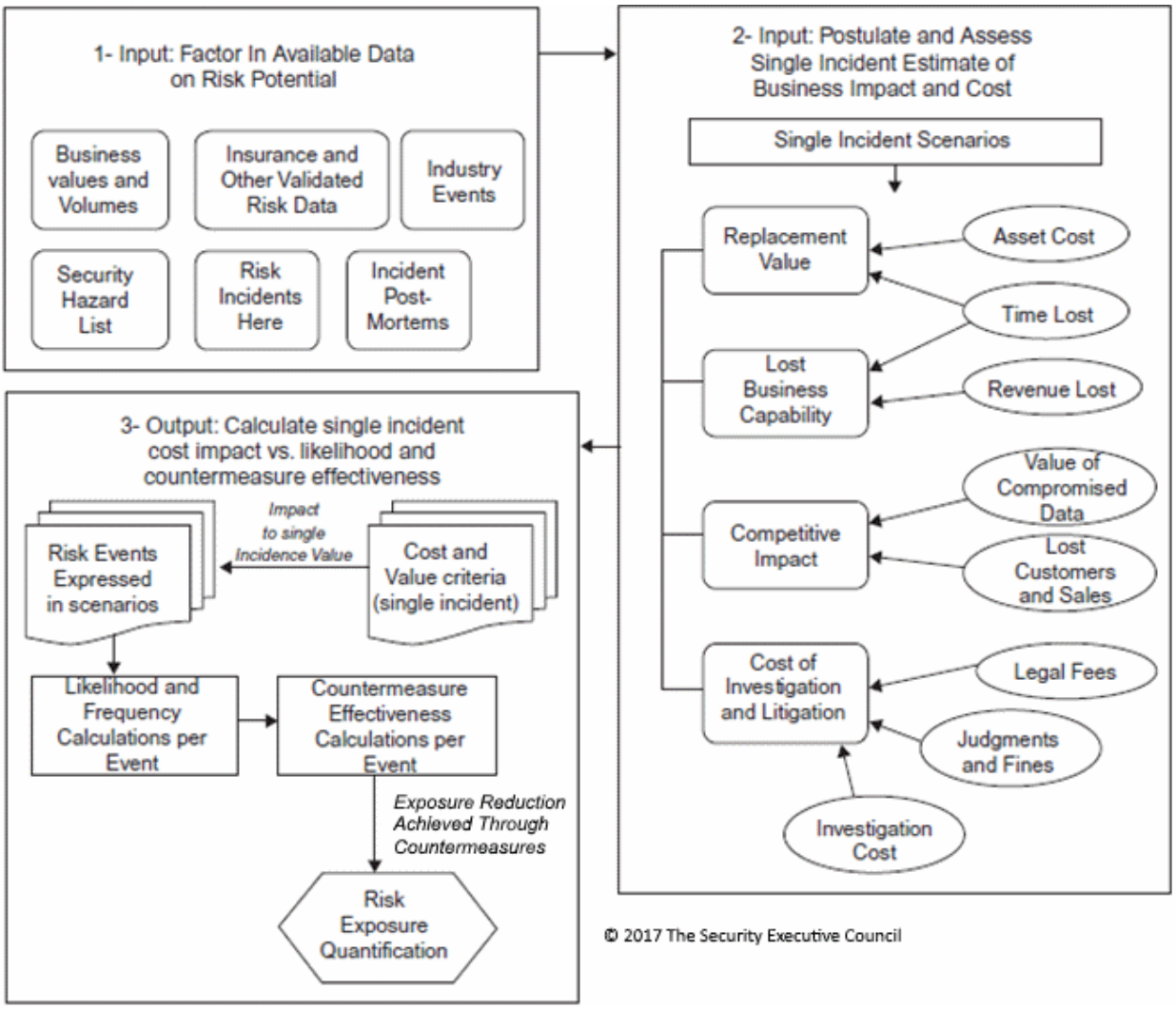
A Risk Quantification Process

Security Executive Council

Having a list of security-related business risks and their associated countermeasures is an essential part of the risk management process. However, understanding how to quantify those risks to set priorities is equally important. The flow chart in the figure below lays out one approach to the analytical process associated with risk exposure quantification.

In Step 1 of the diagram, the process commences with an inventory of business risk information available from internal risk management (values and volume impacts, and insurance data), industry risk data, security's risk and hazard data, known incident data from all governance functions, and incident post-mortem outputs. These profiles enable selection of a more likely set of single-incident risk scenarios. Based on their unique consequences, you now have one or several types of incidents you can value.



Risk Exposure Quantification Strategy—Process Flow. One approach to the analytical process associated with risk exposure quantification.

These scenarios are forwarded to the second step to postulate multiple factors related to the potential consequences and impact of a single incident of the specified type. Estimates of cost may be made for each scenario using a worst-case baseline, such as total loss of a known valued asset, or a less consequential result, such as an outage for a specified time. Impact costs may be estimated by engaging the business unit, which typically has loss-impact data calculations as part of the contingency planning baseline. Other estimates may be merely logical plug-ins supported by prior-event data.

The single-incident cost estimates are then processed through the filter of the effectiveness of the countermeasures that are in place for each risk event. For example, backup resources are in place to respond to a natural disaster outage, and the time to recover may be reliably estimated through prior tests. That recovery time and other impacts may also be reliably cost estimated. You will find your CFO and risk management or insurance offices most helpful in identifying insurance industry data associated with various security incidents, scoping single incident costs to risk impacts, as well as approaches to potential cost to various security scenarios.

Likelihood of an incident is a measure of knowledge of your vulnerability to specific breaches based on test data, known downtimes, audit data on unresolved business process deficiencies, and increased frequency of similar events within your industry or nearby. Effectiveness of countermeasures is also based on test data. The known resilience or identified weaknesses of the countermeasures available in your scenario will drive your likelihood estimates. For example, what if this process were to postulate a much wider impact of the disaster that limited or eliminated the backup capability in our outage scenario above?

You will find that your best likelihood measure used for influential impact will be your periodic testing of the effectiveness of various safeguards applied by your resources and those employed within business units, particularly where they are required by standard or policy. Several key areas of measurement include:

- the perceived value or attractiveness of the object of protection;
- the degree of probable success in penetrating a specific countermeasure; and
- the greater the knowledge of that vulnerability within the population, the greater the likelihood of successful attack.

Each of these concepts may be verified by testing. There are a variety of risk-quantification tools available through risk-management organizations and vendors. This is but one exercise that may be engaged in by a governance team approach or in cooperation with the potentially affected business units.

The bottom line is the need to understand the potential impact of the higher-likelihood risk events in financial and other relevant terms.

The Security Executive Council (SEC)

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of risk mitigation strategy; they strategize with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video or visit our website to learn more: https://www.securityexecutivecouncil.com