White Paper:
Using the Generalized Cost Containment (GCC) Model

By Michael Miora, CISSP-ISSMP, FBCI
President & CEO
ContingenZ Corporation
mmiora@contingenz.com

Table of Contents

ContingenZ Corporation™

Training ▪ Education ▪ Consulting

ContingenZ Corporation
www.contingenz.com ▪ info@contingenz.com

Incident Management: Recognize, React, Respond

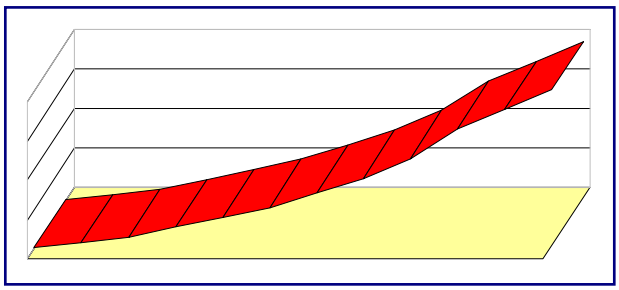
THE ENTERPRISE BUSINESS IMPACT ANALYSIS (BIA)

The Enterprise Impact Analysis is the heart of the Incident Management process. Unlike any threat-based risk assessment, this analysis focuses on the effects or impacts on an enterprise regardless of the cause. The analysis delves into the functions and uses of enterprise elements and evaluates how any interruption or outage will affect proper and normal business functioning.

The impact analysis is the heart of the process.

This analysis provides the framework for determining in the context of an incident what is important and in what time frame and what is not relevant to the managing of an incident. The analysis determines how to best protect the people, information and equipment that constitute the organization and its functions so that all survive the incident to flourish another day. It is here that the planner determines what is important and in how does that importance relate to the recovery time frame. The BIA determines how far to go in protecting the information and equipment that constitute the organization and its functions so that all survive to flourish another day.

The Miora Generalized Cost Containment (GCC) Model is a modern and superior alternative to the older, more conventional threat-based risk assessment methods. The GCC estimates the total cost of outages as a function of time after an event regardless of the cause. When compared with conventional techniques, this model is easier to build, simpler to explain, and less costly to perform. A key factor is that the model estimates the cost of an outage to an enterprise for each function and applies that cost to the total cost only after the maximum allowable down time has been exceeded. It then consolidates that information into a master model that is independent of causes and threats, yet captures whether the loss is tangible and direct, tangible and indirect or intangible.



The GCC can solve the problem of cost justification and demonstrate improved ROI by combining the incremental issues caused by specific threats into an overall Incident Management profile that gives top management a clear vision of what, how and when corporate assets need to be protected.

THE GENERALIZED COST CONTAINMENT MODEL

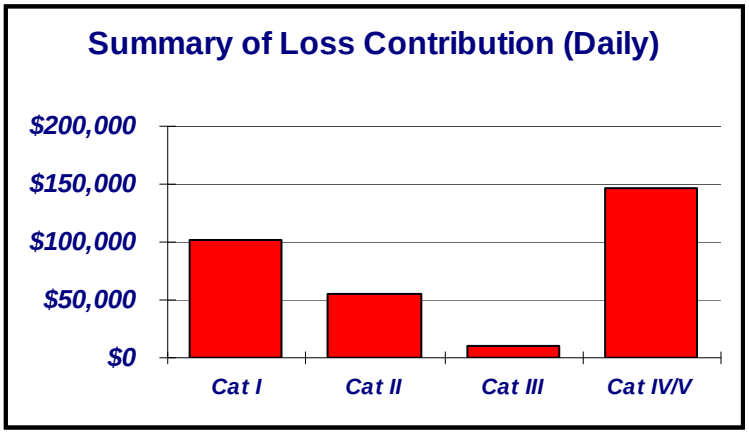
Introduction

The Generalized Cost Containment (GCC) Model rises above consideration of probabilities of specific disaster events; it estimates the total cost of outages as a function of time after an event. This model is significantly simpler than the conventional Quantitative Risk Model: it is easier to build and simpler to explain. The GCC estimates the costs of high-probability outages with sufficient depth and detail to prove the value of the incident management element under analysis.

For instance, assume the cost of delaying the Treasury Department's bank management function is $25,000 per day after the first day and the cost of delaying the Law Department's general contract review is $5,000 per day after seven days. For the bank management function, we calculate the cost to the company as $25,000 per day beginning on the first day. For the contract review function, we calculate the cost as $5,000 per day beginning on the eighth day. Therefore, the contract review function does not contribute to loss during the first seven days. We perform this calculation for each function and collect the costs by category. This category cost summary is used to develop and present a graph that shows the total cost losses for each category level once they are activated and the total for all categories over time.

Categorizing Functions

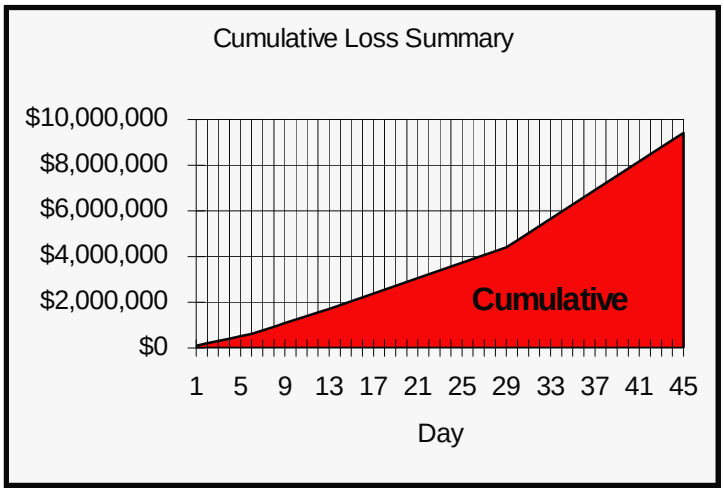
A sample graph of the contribution of functions aggregated by Category level is shown in the Figure. In this example, Category I functions cause slightly more than $120,000 of loss on a daily basis once the maximum allowable downtime has been exceeded. Category II functions contribute slightly under $60,000 in this example. It is likely that functions will commence their loss contribution at various times after the disaster event. Therefore, the true Category I loss contribution may begin at a lower level and increase to its full level. That distribution of effect will occur beginning on the first day any function exceeds its allowable downtime and continue growing until the last day any function exceeds its downtime, at which point the effect will have achieved its full loss contribution. Since the categorization clusters functions with similar downtimes, we can present the loss as a single, or point, value rather than a value that varies over time.



Notice the shape of the set of bars: Category I is a higher value than Categories II and III. Category IV is high. This is a characteristic shape for this graph. No matter the number of categories chosen, the Category I functions tend to be quite high in their contributions. The next one or two categories are lower, but increasing in values until the lowest priority category, which tends to be quite high. This shape results from the manner of the categorizations. The Category I functions are highly critical with great effects on corporate operations. Category I functions tend to number in the few, with each function contributing significantly. The middle categories tend to be larger in number than Category I, with the number increasing with each succeeding category, though still small compared to the overall set of organizational functions. The final category tends to contain the largest number of functions. Though many contribute less on a daily basis than the Category I functions, the sheer magnitude of this set often causes it to be the largest overall contributor to loss. Recall, however, Category I functions begin their effects quickly, while loss of Category IV functions may be benign for weeks.

Accumulating Losses

A sample graph showing the accumulation of losses from all categories following a disaster is shown in the figure. Note that this figure uses the data from the previous figure but in a different format. Neither this nor the previous figure measures physical losses such as real property, capital equipment, and the like. The horizontal axis (x-axis) represents the number of days since the disaster event caused damage and cessation of corporate functions. The vertical axis (y-axis) represents the total losses the company will have sustained on the corresponding day represented on the x-axis.



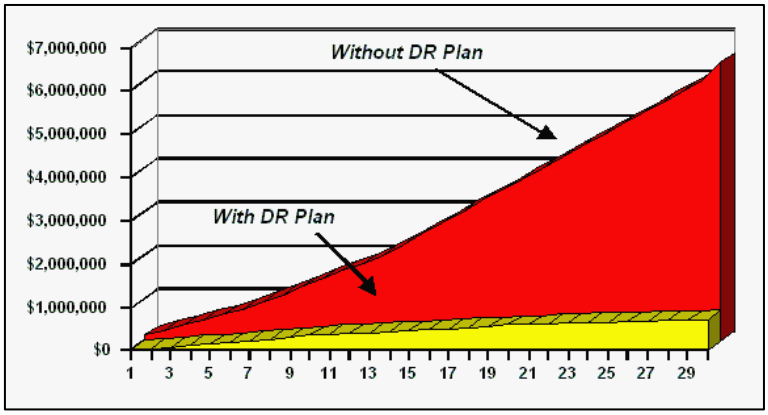
At the point of the disaster occurrence, no losses will have accumulated as the result of the non-performance of any function. Hence, the accumulated loss begins at zero on the first day. Thereafter, the accumulated loss is increased each day by the cost contribution of the category whose earliest start time has already been surpassed. Let us assume that Category I functions begin to contribute to corporate losses of $120,000 on the first day, and Category II functions begin to contribute losses of $60,000 on the seventh day. Further, assume that Category III functions contribute $80,000 daily beginning on the fourteenth day. In this case, the cumulative loss begins at zero and grows by $120,000 per day for the first six days. On the seventh day, the Category II functions begin to con-

tribute $60,000 per day along with the ongoing contribution of the Category I functions. Therefore, beginning on the seventh day, the cumulative loss grows by the sum of $120,000 and $60,000, which is $180,000 daily. On the fourteenth day, the daily loss increases by another $80,000, representing the Category III contribution. This brings the total daily loss to $240,000, which is the sum of the contributions of Categories I, II and III.

The cumulative loss summary shows at a glance the loss the company will experience over time following the disaster if no disaster recovery planning is performed. The active simplifications of this model are the grouping of functions by category and the subsequent representation of each category as a single value beginning at a fixed point in time. This may render the estimate slightly inaccurate at some local points, but the overall values are as accurate as the underlying estimates.

The Generalized Cost Containment (GCC) Model summarizes at a glance the effects of loss of functions. The Law of Large Numbers helps assure that the overall estimate is reliable. These loss figures can be moderated by insurance reimbursements, legal liabilities, and overall management objectives.

A second model can be developed assuming the disaster recovery planning is in place, thereby showing the residual loss proposed. That model would be developed in a similar manner, but with the assumption that certain functions are restored within established parameters. There would be residual loss only if the restoration occurs later than the allowable downtime. This will almost certainly be the case for some functions. The figure illustrates a graph that shows cumulative losses with and without a disaster recovery plan in place. The Without DR Plan curve is similar to the previous figure. The With DR Plan curve reflects the residual loss that will occur even if a plan is in place. This loss is normally dramatically lower, but is seldom zero. Typically, a reduction to zero residual loss would require extraordinary and expensive measures such as parallel processing with real time backup to off site locations. Most organizations can benefit more from a significant lowering of residual losses than from a full reduction to zero losses.



Estimating the Losses

For each function, estimate the loss based on three criteria or types of losses. These three losses are: tangible and direct losses, tangible and indirect losses, and intangible losses.

The tangible and direct losses are the easiest to calculate. These losses can be traced to specific revenue producing functions. The results are direct because the loss occurs as a first order effect, meaning that revenue stops because the function cannot be performed. The results are tangible because they can be easily measured. An example of such a function is automated production control of an assembly line. If the systems exceed their allowable downtime, then production will cease. The cost is the resultant loss of sales after inventory is depleted. Another example is loss of order entry functions. In this case, the result is similarly calculable: lost sales after in stock items are depleted and existing orders are produced. Tangible, direct losses include lost sales, lost manufacturing, lost deliveries, and other lost opportunities.

The tangible and indirect losses are the most common and slightly more difficult to estimate. Support functions generally produce tangible results whose privation would cause a fiscal loss indirectly. For example, a public corporation issues quarterly earnings reports that, if late, could have significant consequences on the company's stock value. Though this is not a direct loss resulting from cessation of sales or other production, the loss can be calculated using accounting standard practices. The internal accounting personnel are in the best position to provide this estimate to the disaster recovery planner. Tangible, indirect losses include penalties, fees, fines, market share, and other issues that can be directly calculated.

Intangible losses are the most difficult to calculate. These intangible effects include reduced public confidence, compromised customer satisfaction, promises not kept, damaged reputation, and other losses that are general in nature and not easily calculable. Sometimes, these losses are not translated into specific fiscal losses and are, therefore, not represented in the cost graphs. In such cases, prominent notations should be make explaining the additional, but not quantified losses.

CONCLUSION

In 2002, the keys to successful incident management are to show the effectiveness of the solution, demonstrate reasonable ROI, and perform analyses that are applicable within a short timeframe of one to three years. Avoiding the paralysis of the detailed analyses that hinge upon low probability events with very high impacts is invaluable to explaining and illustrating the advantages of a unified Incident Management plan to management.