

WHY BC FOR SMEs SHOULD BE DIFFERENT

Author: Kathleen Lucey FBCI, Montague Technology Management, Inc. Published in Continuity, Volume 9 issue 2.

In the wake of the events of 9/11, many executives and owners of small and medium-size businesses began to feel insecure about their futures. Most had only rudimentary Disaster Recovery programs; many entrepreneurs did not start their careers in IT. Many wanted to feel more confident about the ability of their firms to survive such an event.

And yet there has been very little development of meaningful continuity capability in these businesses. Why is this?

We can say that building an effective continuity capability costs a lot of money. This is money that SME's may either not have or not want to spend on such a program. It may also be true that the current approach of the BC industry may not be the most appropriate for their needs.

Maybe we need to look at our current methods and techniques, with a view to adapting them to the perhaps very different needs of SME's. After all, our industry grew and has flourished in a radically different economic sector: financial and brokerage, government and large public corporations, many of which developed a continuity capability in order to meet regulatory mandates. In other words, their spending on continuity programs was not optional. It was a means to avoid fines and other regulatory penalties. And certainly it is common knowledge that the culture and psychology of small companies are significantly different from those of large multinational public corporations and government agencies.

We could also generally agree that the fact that many (and probably close to all) continuity programs originally began their existence within the IT department as a response to a regulatory requirement has colored how our methods and tools have evolved to the present. We might be using very different tools if the BC Industry had begun within the very demanding crucible of the SME, where effective results are required and ROI rules.

This article discusses a few of the historical reasons why what we provide now may not be suited to SME needs, and provides an overview of a different path we could take to provide an approach that will mesh better with both the economic and psychological needs of SMEs.

After all, SMEs are the job-generation engines of the economy, and represent a significant portion of its value. Therefore, as BC professionals, we owe it to ourselves to take this sector seriously, both from a sense of social responsibility and to ensure the continued economic growth and development of the BC Industry.

The Past Is Not the Future....or the Present

There are several primary drivers of development in our industry. Here we will look at the effects of three: government regulations, available market solutions, and the IT birthplace of our industry.

Let's look first at government regulations. These regulations affect primarily the financial and brokerage industries, as well as some pharmaceutical functions, and of course government agencies. These regulations vary by industry and by country, but all aim to ensure a minimal strength of internal controls (the data are correct) and to ensure that critical business processes can, if interrupted, restart soon enough to prevent a loss that threatens the survival of the entity.

If we look at the level of current continuity capability at large banks or brokerages, we see large programs, documented recovery plans, and extensive facilities and plans for technology recovery. What we do not see is realistic testing that takes into account all of the interdependencies: what inputs are required from which internal and external sources, what outputs must be sent to which internal and external partners. We rarely see the kind of integrated testing that would reveal synchronicity problems in the recovery of multiple interdependent applications.

We will probably see extensive business continuity plans by department, but these are generally "business recovery" plans rather than continuity plans. Occasionally we see testing that relocates business functions to alternate space; however, it is extremely rare for these functions to perform their day-to-day work from these alternate locations. It is the extremely rare case where we see an exercise that integrates business and technology recovery together with essential external partners. But it is clear that this is the sector with the most highly developed continuity capability.

A generally shared characteristic of these plans is that they are designed to address the so-called "worst-case scenario," a smoke and rubble destructive event like 9/11. In this type of "unanticipatable" event, planners feel there is nothing they can do to avoid the interruption, so they concentrate on recovery. Since this is the ONLY scenario that is being planned for, these plans generally do not include any measures that would avoid an operational interruption of anything less than catastrophic severity or decrease its probability, with the notable exception of supplemental electrical power sources.

Another driver of BC Industry growth was the early emergence and strength of the large commercial alternate site providers. It is appropriate to remember that this segment of the industry emerged directly from IT: it was a way to re-use IT equipment that was already paid for, having been used for multiple leases. The original "hotsites" were developed using a shared mainframe and storage platform that provided relatively inexpensive facilities for the re-creation of a company's IT infrastructure, shared on a "first-come, first-served basis." It was the ideal solution for meeting regulatory requirements to cover the "worst-case scenario" at minimum cost.

And so it should not be surprising that the earliest continuity programs focused on this business model of IT recovery. The giants of the industry – Comdisco, SunGard, as well as the IT firms that later entered this sector – IBM, HP, Digital, and others -- all grew their alternate site businesses largely on these two premises, “worst-case scenario,” and the sharing of alternate site resources as a relatively inexpensive way for IT to meet regulator requirements.

We also need to look at the ramifications of this term, “worst-case scenario,” which was used extensively by the large alternate site providers to develop their businesses. During the days of the mostly batch mainframe computing in the 70’s and the first half of the 80’s, this was an effective slogan. The early convergence of regulatory mandates for the quick recovery of the data center and this “worst-case scenario” slogan created a bonanza for the early providers of alternate sites. Even in the second half of the 80s it was still a demand-driven sector.

The official interpretation was the following: “If you plan for worst-case scenario, you have covered all other less severe scenarios.” This slogan, however, lost force as the IT industry changed and the commercial alternate site providers had to work harder and harder to find customers. The inexpensive shared resources solution they proposed became considerably more expensive as it became less shareable, as the IT industry broadened and deepened with the move away from mainframes to the application-specific servers, internet, the PC, and decentralized computing that characterize our current environment. Although the alternate site providers continued to rely on this shared resources model because it was so central to the high profitability of the commercial alternate site, new customer deals in fact became less profitable. Customers became more difficult to find because the alternate sites for servers, PC’s, network facilities, and workspace grew more and more expensive --- until other solutions started to look better, or at least as good.

There was also another factor in operation: a dawning realization in the BC Industry that what needed to be recovered was the business, not the IT department. Some have said that the alternate site providers moved away from “disaster recovery” to business “continuity” because “disaster recovery” was such a negative term. Others say that this came about because they were experiencing a slowdown in their business and therefore tried to expand into a larger field. Whatever the term or the reason, the BC industry certainly brought its IT-based recovery tools and techniques into this new sector of business function recovery.

The “worst-case scenario” slogan has become ingrained within the industry, and what had been an extraordinarily effective marketing gambit has become a ruling force. Almost all IT and business function recovery plans still focus on this total physical disaster. If we assume that these plans were designed carefully, and tested thoroughly, they should protect the firm in that most severe and least probable of events ... if it ever happens!

However, such plans, concerned as they are only with those statistically extremely improbable catastrophic events, are not generally used in interruptions of less severity. Nor

can they do anything to mitigate the probability of interruption events that occur at a much greater frequency.

The truism, "If you plan for worst-case scenario, you will have covered all other less severe scenarios," spoken by thousands of business recovery consultants and advisors and coordinators, turns out to have been not true at all. It is even less true in a business environment where multiple resources, some not controlled directly by the business, must all be simultaneously present to execute a complex business function. In this case, the loss of a single resource can stop the operation cold. There may be no smoke and rubble here, but the operational interruption can be devastating nonetheless.

What these plans will not do is extremely important:

- They will NOT help the organization to deal with a less severe but certainly challenging interruption that has a far greater probability than the "worst-case" catastrophic event. Generally, such an interruption will not "activate" the "worst-case scenario" plan.
- They will NOT help the organization to gain greater control over its environment through the use of avoidance and mitigation measures that allow us to monitor conditions to detect an emerging fault, to react through regular maintenance, training, and other activities, and to correct the condition before it produces an interruption.

The best way to recover from an interruption is to avoid it.

SME's are Fundamentally Different from Current BC Implementers

First and foremost, the owners of most SMEs are by definition entrepreneurial risk-takers. Second, they are generally unregulated – at least while they remain privately held. Third, if the owner receives a salary, it is not his/her main source of compensation. In the case of SME revenues – costs = income for the owner's mortgage, for the education of his/her children, for the food on the dinner table, for the owner's LIFE. When you compare this situation to that of the average middle manager (and most commonly the IT Manager or the CIO) who is the decision-maker for BC projects at a large regulated corporation, it is easy to see why the owner of an SME is necessarily more sensitive to spending large sums of money to protect his/her firm from the least probable interruption event, the infamous "worst-case scenario."

By temperament and by culture, the entrepreneur needs to have a tangible, visible, return on investment. However great the profits of his/her company, s/he will balk at spending large sums of money on a BIA that provides analysis but no solutions. S/he knows what goes on in his/her business, knows its critical dependencies. What s/he does not know is how to identify potential interruptions and how to minimize their probability of occurrence. S/he generally is looking for effective results; these need to be made visible and their benefits made clear.

It is easier to respond to these requirements by addressing those interruptions that occur with greater frequency, rather than dealing only with the least probable of interruptions, the

“worst-case scenario.” Looking at the diagram above, it is easy to see that the universe covered by efforts directed at minimizing the more probable interruptions, through programs designed to assure greater availability, reliability, and business process engineering, is far larger than that covered by “worst-case scenario” continuity/recovery efforts.

It is not difficult to imagine why this approach would be more acceptable to the SME entrepreneur.

The Present and the Future Hold Challenges Even for Traditional BC Programs

The methods and best practices that the BC Industry has evolved over the years are geared to the firms and government agencies that fit this model: large public corporations and government agencies that, with few exceptions, are required by regulations to have recovery plans. The Sarbanes-Oxley Act, while not specifically requiring such plans, certainly implies that effective internal controls must be in place to ensure that even otherwise unregulated public companies have the resilience to protect the assets of the shareholders during an interruption event. It does not take a giant leap of faith to see that recovery plans geared only to the least probable “worst-case scenario” will not satisfy this newest regulation.

The tools and best practices that we develop to address the needs of SME’s will be effective for both regulated and unregulated public companies as well as for government agencies – for any business organization. What will those tools and best practices look like and how effective will their results be? We have a lot of ground to cover to meet these current and future challenges. One thing is certain: an SME entrepreneur will not respond well to our traditional IT Recovery methods based on “worst-case scenario.”

I have a few ideas for some different approaches that owners of SME’s might feel comfortable with. And I am sure that you have a few as well. But that is for another committee, another article, another day. In the meantime, I am confident that the BC Industry is up to the task. All we need is to come together and pool our already considerable expertise.

