Wass Consulting Group, Inc.
Management Insight

Management Consultants **Vol. 7, No. 2**

Securing Business Continuity

It's more than just Emergency Planning/Disaster Recovery

Summary

With the events of September 11, 2001 as a backdrop, the imperative to protect the business enterprise from a more diverse array of business risks has never been more apparent. While many of the threats and risks are well known, and have been planned for, companies must shift their thinking from planning for containment and recovery from specific point risks to a far broader and longer term "business continuity" mindset. It is no longer adequate to merely recover from the immediate casualty - the business must quickly and decisively return to full competitiveness in challenging markets, no matter what the calamity. Executive management has the responsibility for identifying and managing business risk, and the Board of Directors has the responsibility to ensure that this is accomplished with appropriate vision and perspective.

Background

Since their formation, utility companies have been keenly aware of the disruptive effects of weather and natural disasters on their operations. Tornadoes, hurricanes, earthquakes, floods, and snowstorms are just a few of the challenges that U.S. utilities have faced and learned to live with over the years. While such challenges have been significant, proper planning and development of emergency response protocols have generally allowed utilities to "weather the storm" and restore service to their customers in reasonable timeframes. In addition, because the very nature of such unplanned events were not foreseeable (other than perhaps in the aggregate over a several year timeframe), they were generally covered by a combination of insurance and/or an understanding Public Service Commission that allowed recovery through a regulated rate structure. Unfortunately, with increasing de-regulation, this regulatory safety net is rapidly fading or for many companies, is already gone.

Subsequently, as nuclear plants assumed a greater role in America's energy mix, Emergency Planning took on a greater significance as generating stations in addition to the transmission and distribution systems came under increased scrutiny. The security of these resources from both natural and man-made threats continues to receive increased attention, and the resulting amount of time, effort, and money devoted to protecting the health and safety of the public in the event of an emergency is enormous indeed.

Ensuring the continued viability of the business is fundamentally different than protecting the health and safety of the public.

Nonetheless, a fundamental change took place on September 11, 2001 when terrorists attacked U.S. facilities in New York, Washington, and Pennsylvania - a change that is only gradually making itself apparent to utility executive management and their Boards of Directors. If

1701 Quincy Ave., Suite 31
Naperville, IL 60540
Web site: http://www.wcginc.com
Toll Free: (800) 601-9277
Phone: (630) 637-1405
Fax: (630) 637-1404
E-mail: info@wcginc.com

natural disasters were difficult to plan for, such man-made acts are even more so.

More importantly, it is becoming increasingly clear that such threats can impact not only utility facilities, but the very fabric of the business enterprise itself. Not only are portions of the distribution system, or the transmission grid, or one or more of the production/generation facilities at risk, but the entire business or significant parts of it could be shut down for significant periods of time.

Recent experience has amply demonstrated such risks, as shown in the table below, as well as pointed to some approaches to possible solutions.

Examples of Recent Threats to U.S. Businesses
▪ World Trade Center disaster
▪ Enron failure, and impact on Arthur Andersen
▪ California energy crisis
▪ Flooding of underground tunnels in Chicago
▪ Hinsdale telecommunications facility fire

Businesses that were wholly located within the World Trade Center were demolished, and many will never be seen again. Of those other businesses that were geographically dispersed, however, some will survive **if** they took appropriate actions beforehand to provide for business continuity in the event of a disaster.

Examples of such firms that may prove successful are several financial trading firms with multiple offices AND who had real-time backup of client-related data located off-site. This should not be misconstrued to suggest that simply backing up important electronic data by itself will ensure continuity of operations following a disaster. Nothing could be further from the truth. For example, while 95% of the data centers affected were back in operation within one day of the attack, only about one-third of the businesses were back in operation as late as six months after it.

While an Information Technology (IT) Disaster Recovery Plan is an obvious element of an overall solution, it is only one part of a broader strategy to ensure business continuity in the event of unplanned events, be they natural or man-made.

Business Continuity Management

While emergency planning and disaster recovery are well known concepts in the American business lexicon, Business Continuity Management (BCM) is less well known. Early proponents of BCM were typically information technology practitioners who were principally interested in recovering data resident in the firm's mainframe computer in the event of a major computer glitch (i.e., a disaster). Unfortunately, some proponents still take this narrow view of BCM. The overblown fears of Y2K difficulties a few years ago had at their heart the valid concerns over business continuity, but again were mainly focused in practice on computer and data processing problems. Today, the strongest proponents of BCM come from Europe, and in particular Great Britain, who have had to face the risk of terrorism and other disasters over the last decade. In general, they have taken a more holistic approach to business continuity in the event of unforeseen threats, and provide a more appropriate model for business continuity than we in the U.S. have seen, except perhaps in the largest multi-national companies. Major elements of the model include:

"Two out of five enterprises that experience a disaster go out of business within five years."

infoworld, October 2001

- **Knowing the business** - identifying its mission critical functions and activities

1701 Quincy Ave., Suite 31
Naperville, IL 60540
Web site: http://www.wcginc.com
Toll Free: (800) 601-9277
Phone: (630) 637-1405
Fax: (630) 637-1404
E-mail: info@wcginc.com

- **Conducting a business impact analysis** - identifying what could happen if the mission critical functions/activities were compromised

- **Conducting a risk assessment** - evaluating the likelihood of negative business impacts occurring

- **Determining continuity strategies** - developing strategies to address the most serious business risks

Knowing the Business

Business Continuity Management is a proactive and continuous process driven from the top of the organization. It identifies the key functions of an organization and the likely threats to those functions. From this information, plans and procedures which ensure key functions can continue whatever the circumstances can be developed, tested, and revised to ensure they are workable when they are needed.

In many cases for which U.S. utilities have developed emergency/disaster recovery plans, the nature of the disaster is generally know from experience (e.g., weather caused) or postulated a priori (e.g., a terrorist attack on a nuclear power plant). Unfortunately, tomorrow's challenges will be far less certain, and likely very different. Therefore, a critical first step in addressing business continuity is to understand your business, and to establish what is vital for its survival. After all, it is on mission critical activities that BCM must focus. In today's utility companies, this focus can generally be placed on one of three levels, including:

- The enterprise level (e.g., a holding company, or the entire corporate organization)

- The operating company level (e.g., a particular key business unit)

- The facility level (e.g., a particular power plant, T&D facility, or building)

Each level has its own mission critical functions/ activities, and planning for/evaluating/ensuring business continuity should be performed separately at each level. Although the overall approach for each level is the same, the details of the effort and the specifics of any plan/implementing procedures would, of course, vary considerably. In fact, the plans/procedures would likely vary considerably even among different units at the same level (e.g., different operating companies/business units or different facilities).

As every organization has many dependencies (both internal and external) that support the mission critical functions and processes, these should be identified near the beginning of the effort. These may include:

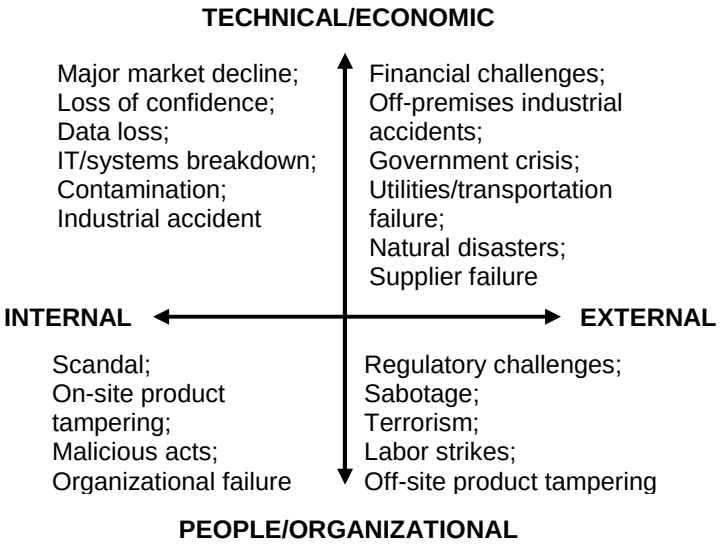
- Internal dependencies - suppliers, customers, shareholders, employees, IT systems, production/delivery processes, support services, etc.

- External dependencies - banks and the investment community, bond rating agencies, regulators, competitors, trade bodies, pressure groups, the press/media, etc.

Once these dependencies have been reviewed, a compilation of mission critical functions and processes can be developed.

Business Impact Analysis

Having identified the mission critical functions and processes, it is important to determine what the impact would be on the organization if these were disrupted, or lost. One way to record where such basic threats may arise is to plot them on a four degree framework such as shown on the following page.



The subsequent evaluation of the impacts on the organization of such threats is often called the Business Impact Analysis (BIA), and enables the organization to focus its efforts on essential business elements rather than conducting a more global (and potentially never-ending) threat-specific analysis. Whatever threats the organization faces, the ultimate impacts are relatively few and often common, all of which produce similar disruption regardless of the specific cause.

Common threats include loss of (at a site, business unit, or enterprise level):

- **Critical systems and infrastructure** (e.g., phones, computers, process controls, HVAC, electricity, water, wastewater,etc.)
- **Access** (e.g., inability to access or occupy key premises, structures, facilities, or sites)
- **Personnel and intellectual capital** (e.g., dead, dying, injured, grieving, dealing with home/family, aging workforce, training inadequacies, labor strife, etc.)
- **Data** (e.g., systems unavailable or delayed, data/records gone or garbled)
- **Market** (e.g., market demand curtailed or disrupted)
- **Reputation** (e.g., overall market available, but not for your firm)
- **External approvals** (e.g., licenses, permits, regulatory actions, legislative changes)

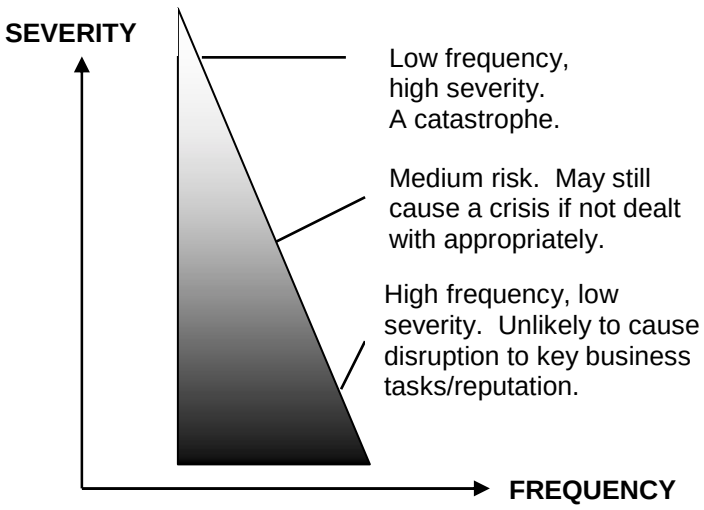
The BIA process should also take into account the time sensitivity of important business functions/ processes to disruption, which in turn will determine recovery objectives. To the extent possible, the impact on the business of various threats should be quantified, either on a subjective rating (e.g., high - medium - low) or scoring (e.g., 1 to 10) system, or with financial values placed on the business impact.

Risk Assessment

Once the major threats and their impacts on mission critical functions/activities have been identified, it is then necessary to evaluate the likelihood of their occurrence, a process that is usually called the Risk Assessment (RA).

If the threats can be described with sufficient accuracy for a calculation to be made of the probability of them happening, such as on the basis of past records, they are often categorized as insurable risks. If the threat is met so infrequently that there exists no way of determining the probability of its occurrence, no underwriter will insure against it and it becomes an uninsurable risk. Either risk, poorly handled, can result in disaster, if only through catastrophic damage to the company's reputation.

As with the Business Impact Assessment, the Risk Assessment should be quantified to the extent practicable (e.g., on a high -medium - low, 1 to 10, acceptable/unacceptable) on a common basis. It is then possible to combine the findings from the BIA and RA to produce a ranking system identifying those areas where planning and recovery resources should be concentrated. A graphic portrayal of the resultant findings is illustrated at the top of the next page.



Continuity Strategies

Having identified those areas where the organization is most at risk, a decision must be made as to how best to proceed, both in terms of protecting physical, financial, and personnel assets, but also in terms of recovery. These could range from doing nothing (e.g., for commercially acceptable low-impact risks), changing or altering existing processes and/or procedures, insuring against the risk, to taking tangible steps to eliminate or reduce the risk through loss mitigation measures. In the most extreme cases, the Business Continuity Plan and its subsidiary Emergency Plans/Disaster Recovery Plans may need to be implemented.

The details of developing a comprehensive Business Continuity Plan (BCP) from the previous analyses are beyond the scope of this ***Management Insight***, and depend heavily on the specific results of those analyses. Obviously, business continuity for a corporate organization would differ markedly from that of one of its individual facilities. What is important at this point, however, is that such plans are developed and put in place; that they are sufficiently comprehensive to address all significant risks; that they are tested, exercised, and audited at periodic intervals; and that the BCP and its subsidiary plans are suitably maintained and revised.

Responsibilities for Ensuring Business Continuity

If one were to ask who is responsible for identifying and managing risks to the company, it is likely that the questioner would get many different answers, depending on the threat postulated. As the potential impact of the threat increased in severity, however, most people would respond that it is the responsibility of management to identify and manage risks, but it is the responsibility of the Board of Directors to ensure that this is accomplished with appropriate vision and perspective.

"The Board of Directors is responsible for the company's system of internal control" ... [which] "depends on a thorough and regular evaluation of the nature and extent of risks to which the company is exposed."

Guidance for Directors on the Combined Code

Although implicitly the case in most U.S. companies, this division of responsibilities has been made explicitly clear in Great Britain. In 1998, the London Stock Exchange issued a document, known as the "Combined Code of the Committee on Corporate Governance", which addressed the management of risks in a corporate environment. This document and associated "Guidance for Directors on the Combined Code" (Turnbull Guidance) require that company boards should carry out formal risk assessment programs and ensure the implementation of appropriate risk control measures. They also require as a condition for listing on the exchange that companies confirm in writing that there is an ongoing procedure for identifying, evaluating, and managing the company's key risks, and that it is regularly reviewed by the Board. While this may not be an absolute requirement for U.S. utility companies in the foreseeable future, the additional risks inherent in not doing so may prove to be imprudent in the long run.

The Wass Consulting Group (WCG)

The principals of WCG have been serving the utility and energy industries for over 30 years, and have lived through the changes the industry has encountered.

Our mission has remained consistently the same, to provide general management consulting services that address the challenges that boards of directors and senior executives face in their daily operations. These include matters of mission, governance, strategy, risk reduction and business continuity management, organization, business process transformation and re-engineering, operational improvement, competitive analysis, due diligence, post-merger integration, market entry, and litigation support, among others.

As a complement to these consulting services, we also provide Executive Search consulting for our energy clients. If we can be of service to your organization in any of these matters, please contact us at your convenience.

Recent *Management Insight* Articles

From time to time, the Wass Consulting Group publishes these *Management Insight* articles on issues of interest to our clients. A listing of the more recent of these articles is provided below. If you or someone in your organization would like to obtain a past issue, either visit our website (www.wcginc.com) or contact us directly.

- **Continuous Improvement** - Transitioning to a More Competitive Environment by Activating the Culture Loop
- **Jointly-Owned Nuclear Operating Companies** - Formation Difficulties and Barriers
- **Jointly-Owned Nuclear Generating Companies** - Formation Issues and Considerations
- **Financial Education and Retirement Planning Programs** - A Needed and Inexpensive Employee Benefit
- **Due Diligence in Acquiring Generation Assets** - What Valuation is Sometimes Overlooked?
- **Outsourcing** - Panacea or a Path to Customer Dissatisfaction?
- **Telecommunications** - Utility Diversification Closer to Home
- **Utility Telecommunications - Part 2** - It May be Now or Never
- **Executive Search in the Energy Industry** - Finding Top Talent Requires Special Search Skills

EFFECTIVE APRIL 15, 2002

WASS CONSULTING GROUP, INC.
is moving to:

1701 Quincy Ave., Suite 31
Naperville, IL 60540

Our phone and fax numbers will remain the same.

1701 Quincy Ave., Suite 31
Naperville, IL 60540
Web site: http://www.wcginc.com
Toll Free: (800) 601-9277
Phone: (630) 637-1405
Fax: (630) 637-1404
E-mail: info@wcginc.com