

November 15, 2006

Business Continuity

Maintaining operations after a disaster requires detailed planning

Since September 11, 2001 a series of disasters has occurred with catastrophic consequences. The most severe events included:

2001: September 11 attacks. *The vulnerability of the United States to a major terrorist attack orchestrated by a foreign entity was suddenly a reality, accomplished by al-Qaeda, who trained terrorists in Afghanistan and planned the scheme in Western Europe. The impact was incalculable and enduring. The threat continues today, as recently shown by the case of Dhiren Barot, a British citizen who converted to Islam. Barot pleaded guilty to conspiring to commit mass murder, and on November 7, 2006 he was sentenced to a minimum of 40 years in prison. The judge stated he planned attacks on the United States and the United Kingdom "on a colossal and unprecedented scale." The terror mastermind planned to attack financial targets in the United States, killing thousands of people in numerous terrorist attacks.*

2003: Widespread Blackout in the United States and Canada. *This massive failure of the electric power distribution system demonstrated how human error can jeopardize vital public services and business continuity.*

2004: Indian Ocean Tsunami. *A deadly wave caused by a phenomenon of nature in the Indian Ocean traveled through Southeast Asian waters more quickly than communication systems were able to give warning. Nearly 300,000 lost their lives.*

2005: Hurricanes Katrina and Rita. *An anticipated hurricane overwhelmed a vulnerable coastline and an unprepared government, inflicting lasting damage. Consequently a world superpower failed to meet the basic needs of its citizens in crisis.*

Will coming years bring more disasters? The terrorism situation has not improved and many believe the conflict has been exasperated due to recent events. Natural phenomena are unpredictable, and some scientific studies suggest that such natural disasters are actually increasing in frequency and strength. Regardless of any suspected changes, natural disasters will always be a cause for concern and definitely necessitate a serious need for business continuity plans.

How can we reduce these vulnerabilities and prevent the catastrophic consequences of terrorist actions and natural disasters? More to the point, who will act? This issue of The Lipman Report focuses on the role of the private sector in reducing public and private vulnerability to disaster. This report addresses policies and procedures to prevent, prepare for, and respond to an extreme event in order to minimize impact and facilitate recovery for business continuity.

Increasingly in an era of terror, reliability means the resilience of operations – their ability to absorb or recover from a shock or attack. Many people assume that the answer is the better design of complex systems. A variety of redesigns in data processing and electronic communications, as well as airport and other security systems have already taken place to increase reliability in the face of terrorist threats. More design changes are planned for electricity grids and air traffic control systems. Recent public discussions of business continuity have focused exclusively on design solutions for problems of business protection and recovery from external threat. Systems designers, top executives, and consumers often operate with illusionary perspectives regarding the reliability and security of critical infrastructures. We all focus on service – its cost, capacity and quality, but tend to ignore the actual institutional infrastructure, the organizational tasks, roles and skills that sustain the service. Policymakers, executives, and technical experts continuously debate the best methods to protect our critical infrastructure against a terrorist attack. Critical infrastructures include our electricity grids, water supplies, telecommunications, health care system, transportation, banking and financial services. In the business world, business continuity has become the focus for this reliability challenge.

(continued on next page)

Business Continuity

Maintaining operations after a disaster requires detailed planning

What are the key vulnerabilities? To what extent must the operation of critical services be centralized and consolidated, or decentralized and dispersed to best protect from assault? Interconnectedness within and across systems means the infrastructures are vulnerable to local disruption, which could lead to widespread failures. At issue is the notion critical infrastructures have discreet choke points of vulnerability. As government officials often assert, the nation's defenders have to be successful all the time to prevent attacks, whereas terrorists only need to be successful once to create chaos.

The business continuity plan

Organizations have always needed to prepare for potential emergency situations, but recent world events have created a need to protect against an unprecedented variety of possible situations. Emergency response plans of the past are no longer effective today, and organizations must now develop comprehensive processes to ensure business continuity before, during and after a major crisis. Business continuity plans include identifying potential losses, maintaining viable recovery strategies, personnel training, plan testing and continual plan maintenance. The modern threats that organizations face today require the formation of an interactive process to assure the continuation of an organization's core activities surrounding a disaster.

The leadership of a company or organization has a duty to stakeholders to plan for its survival. CEOs must be prepared to budget for and obtain the necessary resources to secure company assets. An appropriate administrative structure is necessary to effectively manage a

crisis. Everyone within the organization needs to understand who will make decisions, how the decisions will be implemented and what responsibilities will be assigned to the people involved.

Current business continuity plans should consider the potential for multiple failures, an analysis of system vulnerabilities and interdependencies, and mitigating strategies for the potential simultaneous losses of telecommunications, data, control and monitoring systems. Companies must have the pieces in place to conduct real time, worst-case scenario analysis on thousands of contingency combinations. A plan must be in place to respond to multiple credible disturbances. In addition, organizations must ensure that the onsite officials have internal and external authority to respond to crises immediately, without seeking additional management approval. The single most important form of loss mitigation is business continuity planning. The Business Continuity Forum in England estimates that diligent continuity planning can reduce the economic impact of a terrorist attack by a remarkable 50 to 90 percent. Not surprisingly, the Department of Homeland Security website for guiding businesses in their preparedness measures focuses almost entirely on post loss continuity planning and emerging action planning. Additionally business continuity planning is one of the "material risk" controls required by the Sarbanes-Oxley Act of 2002.

Disasters are essentially of three types: natural, technical, and terrorist-caused. These three sources of possible disaster may also be interdependent or occur in combination. The management policies and resources for mitigation and response to dealing with each of them have

much in common. Firms can establish extra operations capacity, evacuation plans, business interruption plans and liability protection that can be used effectively for all three types of catastrophes.

Creating a Business Continuity Plan

Organizations must assign accountability and responsibility to the appropriate staff. The senior leadership must sponsor the creation, maintenance, testing, and implementation of a comprehensive business continuity plan. Making a business continuity plan a top priority for executives will signal to all other employees the critical importance of such a plan. The continuity plan is divided into two main components: a risk assessment and a business impact analysis.

A comprehensive risk assessment is required to identify and analyze the risks that could potentially impact an organization. The assessment must ascertain both the type and the likelihood of any catastrophes. Potential threats should then be prioritized by the probability of an occurrence as well as the level of impact such an event would have on the organization.

A thorough business impact analysis is also recommended. This should be a management level financial analysis that identifies the impact of losing an organization's resources. The analysis measures the effect of resources loss in order to provide reliable data upon which to base decisions on mitigation, recovery and business continuity strategies. In the age of globalization disruptions to the supply chain could come in many forms, from the potential avian flu pandemic to repairing levees on the upper Mississippi. On the surface, these activities do not always appear to be disruptive, but extensive analysis shows that they can cause millions of dollars in losses due to business operations interruptions.

In addition to evaluating external factors, a

business continuity plan must also include the evaluation of internal factors. The most critical processes in the organization must be identified and analyzed to rank the processes in order of importance for business operations.

A wide range of outcomes can develop in the aftermath of an emergency, and a business continuity plan must examine multiple scenarios to assess the impact on stakeholders, finances, and the organization's image. A crisis impact evaluation must also include an estimation of the duration of the emergency situation and subsequent effects. Even the time of the year may be critical in some cases and should be factored into any risk scenarios.

After gauging all these factors, a business continuity plan should address what resources are required for the business to resume functioning, as well as outline several ways to obtain such resources in the event that supplies are limited or obliterated during a crisis. It is important to prioritize these resources as well. Business records are generally one of a company's most valuable possessions and should be stored or backed-up in a safe and accessible location. A plan should include a system for procuring computer hardware and software, specialized equipment and facility space.

Creating and sustaining a crisis management team

A solid and reliable administrative structure is a key component of the total business continuity plan. An organization needs clear definitions for a management structure, authority for decisions and responsibility for implementation. To form an effective crisis management team, members must be selected from nearly every department, especially human resources, information technology, facilities, security, legal and other departments that have been evaluated as a priority for the organization.

(continued on next page)

Business Continuity

Maintaining operations after a disaster requires detailed planning

It may be necessary to form a second tier of crisis management teams in each of the critical departments, especially for larger organizations. The formation of these teams depends on the size and type of the organization, the number of employees and the locations of offices and operations. Any second tier team must have a plan that is consistent with the overall business continuity plan. Ideally, a secondary plan should be defined within the broad plan. The flow of information is critical during emergency situations, so it is important to maintain accurate, up-to-date contact information for all members of crisis management teams.

Recognizing the early stages of a crisis

Within an organization, some departments or functions are particularly situated to observe warning signs of a crisis before an emergency situation has fully advanced.

Many disasters, especially natural disasters, are inevitable or beyond the control of an organization. Recognizing the warning signs will not prevent such disasters, but can make the situation more manageable when a state of emergency develops.

All employees must understand their responsibilities in reporting potential crises. A documented reporting structure is useful to track any trends that are warning signs of a disaster.

An imminent or highly likely crisis, once identified, must be reported immediately to a supervisor or member of the crisis management team. Redundancies must be built into notification systems, as these systems could plausibly be affected in a disaster.

The problem and its severity must be specifically identified as soon as possible. The potential for escalation must also be carefully

estimated. The point at which a potential disaster becomes an actual disaster should be defined by very specific and controlled criteria, and the responsibility for declaring a disaster should be assigned. The business continuity plan needs to identify which activities can begin in the potential disaster stage, and which activities should be delayed until a true emergency has arisen.

The Time for Urgency is Now®

A business continuity strategy is a cycle of planning, testing and revising. Meticulous plan administration and maintenance, in addition to any catastrophes, will expose vulnerabilities that necessitate revisions to the plan.

A risk assessment and business impact analysis provide the foundation for a company's entire business continuity plan. These analyses should be repeated regularly, especially after any implementation of significant changes to the organization's operating environment. Succinctly, the required tasks for business continuity are assigning accountability, performing risk assessments, conducting a business impact analysis, agreeing on strategic plans and the development of a crisis management and response team.

A national effort to reduce infrastructure vulnerability to high consequence terrorism or natural disaster may falter if too many years pass without a major catastrophe. Sustainability may also be threatened if effective protection depends on a level of international cooperation that disintegrates in a time of crisis. The most important element to enhance the public commitment to business continuity is a strategy that encompasses industrial, technological and regulatory advances.



The Lipman Report Editors