BIZPHYX®

business optimization

WHITE PAPER

A Guide to Proactive Business Continuity Planning

Robert Clancy
Sr. Vice President

Executive Summary – Even in the wake of September 11, 2001, little has been done to improve the ability of companies to function in the face of threats to their infrastructure and employees. This paper outlines the state of preparedness, the cost of being unprepared, obstacles to developing business continuity/disaster recovery plans, and basic steps and resources for developing such plans.

BACKGROUND

Recent history is filled with examples as to why companies must develop and maintain effective business continuity and disaster recovery plans. The September 11 catastrophe, the 2003 power blackout in the northeastern USA and Canada, and Hurricane Isabel destroyed facilities, ruined data infrastructure, and compromised employee safety – resulting in huge losses.

These incidents should have been a wake-up call for managers, but companies have been surprisingly slow to react. A recent USA TODAY article quoted a Harris study saying, "A survey of 52 high-ranking executives of *Fortune* 1,000 companies, such as CEOs, chief operating officers, and chief information officers found just 15% said they were prepared (for a major disaster). The average 'preparedness' grade executives assigned to their companies was a C+." [i]

A similar Info-Tech Research report revealed that 60% of the businesses it surveyed did not have a formal disaster recovery plan in place to help deal with the recent blackout.[ii] A recent Computerworld article further reports that while interest in disaster recovery systems peaked after the terrorist siege, IT managers have yet to follow through on many of their intentions.[iii] A Gartner study reports that one in three U.S. businesses would lose critical data or operational capabilities if struck by a disaster.[iv]

COST OF PROCRASTINATION

Estimates of the cost of system down time vary but regardless of the source, it is a huge number. USA TODAY reported that "the typical large company would lose $400,000 an hour with systems down, such as systems that coordinate the entire business from the time raw materials come in the door to the time customers pay, according to SunGard, which provides disaster recovery services. It estimates that a major disaster would last 35 hours. Even if it were 10 hours, it would cost the typical big company $4 million."[v]

A study by Strategic Research Corporation, a Santa Barbara, California, market research and consulting firm, shows that the financial impact of a major system outage can be enormous: consider $6.5 million per hour in the case of a brokerage operation; or $2.6 million per hour for a credit-card sales authorization system.[vi]

What would your company lose if disaster struck? Without a business continuity/disaster recovery plan your company could be out of business. The previous examples cited contemplate *only the loss in dollars per hour of system down time*. But there are costs beyond just loss of data. What would happen if disaster went beyond data recovery as it did on September 11,' 2001, or as a result of the Federal Building bombing in Oklahoma on April 19, 1995? What if an earthquake struck or a tornado wiped out your facility?

Where would your employees report? How would you continue to serve your customers? Who would restore telecommunications and data communications? How would you deal with the media? These are questions that should be answered above and beyond simple data loss.

BARRIERS TO IMPLEMENTATION

So, why do companies put off business continuity/disaster planning? There are many reasons. Perhaps one of these applies to you.

Lack of Strategic Focus

Many managers are so concerned with critical day-to-day business issues they overlook the company's ability to stay on line in the event of a disaster. Business Continuity Planning is overlooked just as frequently as the development of consistent quality and customer satisfaction processes. While many systems focus on quality management like Malcolm Baldrige, ISO 9001, and others, there is only one quality management system, TL 9000, which addresses both the business process and disaster recovery components. TL 9000 is the ISO 9001 based telecommunications standard that requires registering companies to maintain a documented disaster recovery plan.

Insufficient Understanding of Recovery Procedures and Costs

According to George Symons, CTO of Legato Systems, a storage management vendor, businesses need to clean up the basics (in data systems) before they even start to worry about disaster recovery. Most companies cannot even recover data locally. Furthermore, there is often a disconnect between what CEOs think is in place and what IT managers have actually installed. CEOs tend to be unrealistic about how quickly they can recover. In the Harris poll, CEOs and other executives said their applications and data could be recovered in 10 hours, whereas IT managers said it would take as long as 30 hours, representing a $400,000 difference in losses.[vii] On the other hand many CEOs tend to think it's all but impossible to prepare for a worst-case scenario.[viii]

Limited Top Management Backing

Senior management tends to delegate disaster recovery and business continuity to mid-level managers, and accountability is lacking. USA TODAY reports that executives admitted during the Harris survey "that the topic of a major communications disaster has never been discussed at the board meetings of one in five *Fortune* 1,000 companies." [ix]

Shortcomings in Existing Recovery Plans

Many plans concentrate too heavily on data loss and ignore other elements such as facilities and especially, people. According to Ken Walters, Senior IS Director, Public Broadcasting Service in Alexandria, Virginia, "you spend a lot of time to get your systems up in a couple of days…we need to worry about all the staff here, how to provide telephones, coffee pots, desktop computers, things like that."[x] Other times, plans are developed, put on the shelf, and rarely communicated to employees.

Unrehearsed Plans and Procedures

Plans should be rehearsed at reasonable intervals to ensure that what looks good on paper actually helps an organization recover from an event. While each organization needs to decide what is reasonable, plans should be rehearsed at least annually. Lessons learned should be documented and action items assigned to individuals or teams to improve the plan. If a company has an established quality management system, these lessons learned should be tracked to closure through the company's corrective/preventive action system.

Inadequate Plan Review and Updates

Successful business leaders know how to be flexible to address changing markets. The same principles apply to business continuity planning to counter changing threat levels and type. Management review should ensure that lessons learned from rehearsals are considered and implemented, threat levels re-evaluated, and adjustments made as needed. Top management should also review the plan in order to provide strategic guidance, influence the development of the plan, and remain well informed as to necessary improvements to the plan.

A company with a TL 9000 Quality Management System will do this routinely since TL 9000 requires both a disaster recovery plan and regular reviews of the quality management system by *top management.*

DEVELOPING A PRACTICAL PLAN

1. **Start small** – Begin with the basics and expand the plan as you progress. This strategy isn't an excuse not to address all essential elements quickly. Rather, it prioritizes elements, addressing the most critical ones NOW, and the less important ones in a phased manner.

2. **Conduct a detailed threat analysis** – Put together a small team to conduct a gap analysis based on a realistic threat assessment. Develop or purchase tools and expertise to help analyze, categorize, and prioritize threats that are most likely to affect your company.

3. **Assign risk owners** – Assign a risk owner for each threat area. Since risk owners will inherit the planning for their area they should be subject matter experts on the operation. This may include both functional managers and/or individual employees.

4. **Review the gap analysis and plan** – If your company is large, develop a team comprised of risk owners. If you and your partner *are* the risk owners, team up and review the threat assessment, adding to it as you meet together and brainstorm ideas.

5. **Include all elements of facilities and infrastructure** – One of the common errors is to limit the planning to IT infrastructure alone. The plan should address the threats to physical assets such as buildings, inventory, customer property, and employees.

6. **Review the plan** – Once the plan is developed, it should be reviewed regularly. Threats are to be reassessed and plans adapted accordingly. Top management should also review the plan to ensure its effectiveness. We recommend that plans be reviewed at least annually.

7. **Rehearse the plan** – Having a good plan is a step in the right direction. Rehearsing the plan, documenting successes and failures, and making continual improvements are key to ensuring that the plan actually works when disaster strikes. Your planning team can act as an ongoing maintenance team to ensure that corrective actions are implemented.

8. **Communicate the plan to all employees** – One of the biggest mistakes companies make is putting the plan on the shelf. Your plan should be communicated and understood by all your employees.

HOW MUCH IS ENOUGH?

The extent of planning depends on the nature of threats to the organization. It helps to view threats holistically according to organizational profile, type of business, geographical locations, employees, and others. Some factors to consider are:

- **Organizational Profile** – Is the organization a multinational entity with executives who travel abroad? If so, the threat to those employees and the consequences of harm coming to them should be considered.
- **Type of business** – Does the company make hazardous material? Threats to plants, equipment, and employees should be taken into account.
- **Geographical Locations** – Are the company's facilities located in storm or earthquake zones? Are some facilities located in a country where violence is common?
- **Employees** – Does the company adequately screen new employees? Does the company offer assistance for employees who suffer stress and other destabilizing problems? Is there sufficient security to prevent employee theft of data?

In order to develop a plan that is effective, yet affordable, management needs to systematically estimate the kinds of risks and their likelihood of occurrence. A company that makes paper products, with one location in rural Alabama, is very different from a multinational corporation with a headquarters in a major metropolitan area. A company with locations only in the United States faces different risk levels than a multinational company with worldwide offices.

The following table illustrates how to categorize risk factors by weighing individual threats and summarizing them to provide a big picture review.

Company A – Headquarters, Midwest, USA
Risk Summary

Category	Facilities	Data and Information	Employee Health and Safety	Organizational	Total
Weather Related Disasters	3.5	3.5	3.5	3.5	14
Terrorism/Criminal Activities	2.0	2.0	2.0	2.0	8.0
Malicious Acts	1.0	1.0	1.0	1.0	4.0
Proximity of manmade hazards (pipeline, airports, ports, railroad tracks)	4.0	3.0	2.0	1.0	10.0
Health (diseases, etc.)	1.0	1.0	2.0	1.0	5.0
Product related	1.0	1.0	1.0	1.0	4.0
Total	**13.5**	**11.5**	**11.5**	**9.5**	

Using a rating system of one to five, with five being the highest, management can view the risks to the company and develop a plan based on a reasonable threat assessment. The higher the total score, the more detailed the plan may need to be.

GETTING HELP

Government and Private Organizations

There are a variety of resources available to help organizations create effective business continuity plans. Government organizations like FEMA (http://www.fema.gov), the newly launched Department of Homeland Security (http://www.dhs.gov/dhspublic/), and private organizations like Global Security (www.globalsecurity.org), provide disaster planning information and updates regarding active disasters and threat possibilities.

Consulting

Consultants can bring tremendous value by helping companies plan, develop, inspect, and manage a business continuity and/or disaster plan while sustaining focus on their core business. A consultant also offers the advantages of objectivity and specific expertise through the various stages of planning and implementation.

Bob Clancy is Sr. Vice President of BIZPHYX Inc., a company specializing in preparing companies for TL 9000 registration as well as providing process consulting, training, and documentation services exclusively to the telecommunications' industry. Bob has over 35 years in telecommunications and has successfully led organizations in numerous QPA's, ISO 9001, and TL 9000 audits and assessments. For more information on business continuity/disaster recovery planning, or Quality Management System implementation contact Bob at bclancy@bizphyx.com

[i] USA TODAY, Del Jones, August 4, 2003, http://wwww.usatoday.com/money/companies/management/2003-08-04-preparedness_x.htm

[ii] internet.com, staff article, August 22, 2003 http://siliconvalley.internet.com/news/article.php/3067291

[iii] COMPUTERWORLD, Deni Connor, Network World, September 9, 2003, http://www.computerworld.com/securitytopics/security/recovery/story/0,10801,84732,00.html

[iv] COMPUTERWORLD, Connor.

[v] USA TODAY, Del Jones, August 4, 2003

[vi] White Paper, IBM Business Continuity: New risks, new imperatives, and a new approach, 1999

[vii] COMPUTERWORLD, Deni Connor, Network World, September 9, 2003, http://www.computerworld.com/securitytopics/security/recovery/story/0,10801,84732,00.html

[viii] USA TODAY, Del Jones, August 4, 2003, http://wwww.usatoday.com/money/companies/management/2003-08-04-preparedness_x.htm

[ix] USA TODAY, Jones.

[x] COMPUTERWORLD, Deni Connor, Network World, September 9, 2003, http://www.computerworld.com/securitytopics/security/recovery/story/0,10801,84732,00.html