Communications of the Association for Information Systems

Volume 8 Article 30

June 2002

Business Continuity Management

Jeffrey A, Hecht
Word and Brown, jhecht@wordandbrown.com

Communications of the Association for Information Systems

BUSINESS CONTINUITY MANAGEMENT

Jeffrey A. Hecht
Vice President of Information Technology
Word and Brown
jhecht@wordandbrown.com

ABSTRACT

This paper views Business Continuity Management as a progression from more traditional Disaster Recovery Planning. While recovery presupposes an event that causes a failure, continuity suggests the avoidance, or at least minimizing, the impact of a failure. Business Continuity Management is not just about Information Systems. Rather it is about ensuring that the critical business functions can continue. Business Continuity Management is a process not an event and should deal with any threat that could affect the business. For many organizations reliant on sophisticated Information Technology, adequate Business Continuity Management is a basic requirement.

Keywords: business continutity management, disaster recovery planning, managed high availability, continuous availability strategies, recovery window, secure hot site, business continuity planner

I. INTRODUCTION

A Short Personal History

Like many IT professionals who have been around for a few years, I have seen an evolution in awareness and requirements about what was called Disaster Recovery in the past and which is now called Business Continuity Management. My first exposure to Disaster Recovery methodologies was in 1988. I was working for a medium sized, privately held, financial services company one of whose customers was Manufacturers Hanover Bank. We were running a bankruptcy management application for the bank and everything was going well with this large and profitable customer until one of their EDP auditors came out to review the operation and wanted to see our disaster recovery plan. Our meager attempt to explain what we would do in a disaster was not persuasive to the auditor and our large customer demanded we put an adequate plan in place in 90 days or lose the lucrative contract. Inasmuch as I was an IT Director at the time and anointed as the company's Disaster Recovery Coordinator, I started my exposure to this special niche in the IT world.

The first Disaster Recovery plan we built was bare bones by today's standards. Our recovery window was 48 hours and we concentrated on bringing the IBM mainframe processing back up. One day's data loss was considered acceptable and while we did do some planning that involved how we would get key manual processes going if we lost our whole building, we were really just trying to get the system back up and have some data we could enter. We contracted with Sungard Recovery Systems as a hot site backup provider and conducted 2 tests a year, which

involved only IT personnel. While we met the immediate goal of holding onto the Manufacturers Hanover contract, we were really only minimally protected, particularly since our building was adjacent to an international airport. The realization emerged within the company that what we were doing was not sufficient.

In 1993 our medium sized company had purchased a much larger division of another financial services company. As a result, we acquired a high availability requirement. By this time I was the CIO and it fell to me, not just from a disaster recovery perspective, but also as a continuity requirement that we be up as close to 100% of our business hours as possible. Our key systems ran primarily on UNIX platforms at two separate data centers. We built some internal redundancy and made an attempt to build a self-healing network. The technology at the time did not allow that to be fully successful but did make a smaller recovery window realistic. Our recovery target was 30-minutes and we were able to switch over successfully on two occasions. Since the estimated cost of being down was in the neighborhood of $25,000 an hour, we felt pretty good about our efforts. Whether we realized it or not at the time, we'd moved quite a ways up the Business Continuity continuum.

In 1998 I moved on to a .com startup that was originally in the business of delivering high speed Internet access via satellite. As our product line developed it occurred to me that our VSAT[1] product moving TCP/IP Internet traffic could easily be adapted to be a point-to-point backup for a corporate network. By using BGP[2] routing techniques we were able to design an automatic fail over, sub-minute recovery system with near zero data loss. This solution was true high-availability business continuity. The company was working on partnerships with providers I had contracted with in the past, specifically Sungard and Wang Recovery. I was in the forefront of the movement from mere Disaster Recovery to true Business Continuity Management!

We all know lots of .coms failed and even with the niche not directly related to the Internet, ours was among the casualties. As perhaps the ultimate irony from a Business Continuity Management standpoint I now find myself leading the IT organization in a medium sized, privately held, financial services company. Our current Disaster Recovery window is 72 hours, the centerpiece of the plan is to "get the servers up" with little concern for people or process. We contract with Sungard for hot site backup. The realization within the company is that what we're doing is not sufficient. Somehow, I slid quite a ways back down the Business Continuity Management continuum.

II. DISASTER RECOVERY TO BUSINESS CONTINUITY MANAGEMENT

Regardless of the realities of my current situation, my experiences trace the changes in what is demanded by business today. Recovery used to mean mainframe and data center. Since most users were local to the data center, the primary objective was to retrieve tapes and reestablish host computing. A typical recovery window was 24 to 72 hours and one day's data loss appeared inevitable. Some disruption in the business was expected and the basic goal was to recover mission critical computer functions in a disaster environment, supplemented by increased manual processes. The most common method used was a contract with a secure hot site vendor, like Sungard or Comdisco.

For many businesses today recovery is insufficient. The goal is continuity. Recovering host systems is not enough because connections with the Internet, customers, suppliers, remote users and other trading partners are requirements for the business to function. Acceptable windows to recover are measured in minutes not days or hours. Zero or near-zero data loss is often required. In many cases the goal is instant, seamless recovery, largely undetectable by customers. Clearly a plan that anticipates sending for offsite tapes and moving personnel to a traditional hot site environment does not meet these criteria. To achieve the goals, an investment in high-availability solutions and sophisticated network management is required.

Business Continuity Management is one thing you can't really buy - you have to do it. You can purchase meaningful tools and planning help, but in the final analysis you must make it part of the organization or it will quickly become outdated and create a false sense of preparedness. Focusing on the technical challenges described above can obscure the key

[1] Very Small Aperture Terminal, basically a small satellite dish.
[2] BGP = Border Gateway Protocol

element. Business continuity is a *business* issue. As shown in the next section, it requires solving business problems some (but not all) of which are IT problems.

III. KEY BUSINESS CONTINUTITY ISSUES

Business Continuity Management is not just about Information Systems. As the name implies Business Continuity Management is about ensuring that the critical business functions can continue. It's like going down the rapids in an inflatable boat; you tie down what is vital and prepare to lose the rest. Ideally this metaphor would suggest that Business Continuity Management should be business based rather than IT driven, but as a practical matter IT is likely to be required to provide leadership. Some CIO's would argue that you cannot be successful without a senior business manager as the sponsor of the endeavor. Others would argue that the CIO is a senior business manager and should not shirk this duty. My own view is that IT needs to take a leadership role, adequately plan for the disaster recovery aspects of the systems, provide the appropriate level of high availability for continuity and raise the consciousness of the enterprise to the issues; many of which are clearly outside the traditional responsibility of the CIO.

SPONSORSHIP

Whether sponsorship comes primarily from inside or outside IT, the level of commitment to the process must be significant. Continuity is one of those things in business that can easily be shoved aside in the day-to-day struggles to meet deadlines and perform "normal" duties. To be successful Business Continuity Management must count on strong support and a clear understanding of the value to the organization. The commitment must be reflected in the actions of senior personnel as an ongoing commitment to the project. The key element of this support is to drive the importance down through the management chain. Middle managers can dilute the message and effectively disable the program with passive resistance.

RISKS

Business Continuity Management, Information Security Management and Information Risk Management all share many of the same fundamental business aims. All seek to:

- increase business resilience,
- decrease recovery times,
- decrease the threats on business activities, and
- ensure the business can continue to function and sustain acceptable performance.

Business Continuity Management should deal with any threat that could affect the business, focusing on those threats that represent the highest potential risk, including:

- Intentional human threats (hacking, terrorism, sabotage, product tampering)
- Unplanned human threats (error)
- Natural threats (earthquake, flood, hurricane)
- Unnatural environmental threats (blackouts, arson, network outages)
- Commercial threats (unfavorable PR, product problems)

Clearly many of these areas are not ones in which IT people have expertise, although each of these threats can affect areas in which they do.

PROCESS

Business Continuity Management is not an event, it is a process that must change and adapt with the organization. The plans must be able to evolve at least as quickly as the enterprise; ideally plans anticipate and shape change. To be sustainable and resilient enough to accomplish these goals, the firm must make an ongoing commitment to education and awareness. Business Continuity Management also demands a well-organized approach to visibility and change control

since a change in any of many different areas (e.g., organizational, business objectives, technology, or stakeholder expectations) can have major implications to the viability of any plan.

IV. THE ROLE OF THE BUSINESS CONTINUITY PLANNER

The point person in a successful Business Continuity Management initiative is the Business Continuity Planner. Several associations are dedicated to furthering information sharing and formal training for this discipline. Some provide certifications such as CBCP (Certified Business Continuity Planner) and MCP (Master Contingency Planner). Trade publications are dedicated specifically to the niche, the two largest of which are *Disaster Recovery Journal* and *Business Contingency Planning*. Larger companies may dedicate one or more people to this function, but many smaller firms find themselves in a position similar to the one I described earlier about my first exposure to the topic, in which someone is given this responsibility as an extra component of their primary job. While this situation is probably not the optimum, it often is the reality of what is possible.

TASKS

Whether the planner is a dedicated resource or has to carve out time from another primary responsibility, the Business Continuity Planner should seek to fulfill the following tasks:

1) **Lead sponsors in defining objectives, policies and critical success factors.** Leadership requires negotiations to answer the hard questions about:

   - exactly what needs to be done,
   - what the business can afford to do (and afford not to do),
   - how to measure the results and
   - what the total scope and objectives will be.

   Without some success at this step it is difficult to maintain the ongoing commitment at the top level of the organization. If the sponsors don't believe in the value of the goals, they will not support them.
2) **Coordinate and manage the Business Continuity Management Project.** Depending on the organization, this task can include working with a steering committee, a project task force, or directly with the day-to-day business management. This step should also include conducting a Business Impact Analysis and a Risk Analysis.
3) **Oversee the Business Continuity Management project through effective control methods and change management.**
4) **Present (SELL) the project to management and staff.** Selling the project is one of the most important roles for the Continuity Planner. It is so easy for a project like this to start off with a bang and slip into irrelevance. The Business Continuity Planner must continually resell the value of the effort to the organization and keep the need to have an up-to-date viable plan, and the danger of not having one, on everyone's radar.
5) **Develop the project plan and budget**. In addition to the IT related Disaster Recovery aspects, develop the specifics of escalation, notification and activation procedures. Identify vital records and validate off-site storage programs. Devise a personnel control program and data loss limitations. A basic sample plan can be found at : http://www.drj.com/new2dr/newbies.htm
6) **Define and recommend the project structure and management.** In a smaller organization the Business Continuity Planner may be the structure and management.
7) **Manage the process.** Develop test scenarios and enlist the business units participation. Ensure adequate training is provided at all levels. Regularly review criteria and actively communicate to stakeholders.

V. ADDRESSING CONTINUITY VERSUS RECOVERY

Much of the previous discussion could as easily be related to traditional Disaster Recovery as Business Continuity. After all, you need to plan, get top level buy in, adequately

assess and minimize risk, budget, manage, establish suitable recovery windows and test a Disaster Recovery plan. So what are the key elements that differentiate Business Continuity? Recovery presupposes an event that causes a failure. Continuity suggests the avoidance or at least minimizing the impact of a failure. In some sense it's a matter of degree rather than a clear difference. From a strictly Information Technology standpoint, (admittedly already acknowledged in Sections II and III to be insufficient for "real" Business Continuity but nonetheless instructive) the two primary requirements for continuity are

- Availability, and
- Connectivity.

AVAILABILITY

Can you get to the data, process it, and provide it where it needs to be to continue to run the business?

In a typical disaster recovery scenario you lose access to the data and therefore your ability to conduct business for some period of time. You probably have lost forever at least 12 hours of data since that is the average age of your most recent offsite back up[3]. Moving from a traditional disaster recovery mode to a business continuity approach is possible with today's technology but can be expensive. Consider Table 1, put together with information from data put on the Web by Sungard (http://www.recovery.sungard.com/home.cfm)

As you move from left to right through the table, you obtain increased real time data availability and disaster tolerance. You also lower risk, but at what can be a very significant cost. This tradeoff is really what Business Continuity Management is all about, balancing what the business needs to function against the cost of providing it. In some cases the tradeoff is complicated by the fact that you hope you never have occasion to execute the plans you make.

CONNECTIVITY

In the contemporary business environment, available data does not do much good if you cannot share it with your trading partners. The problem becomes more complex as your connections become ubiquitous. The days of direct proprietary connections or a dial-up to a Value Added Network are largely gone, replaced in many cases with an Internet connection. The connection may be your own Web site or a portal or a consortium trading venue of some kind. Customers expect that Web connections will always be available. To provide that kind of availability fully requires a physically diverse network with multiple connections and sophisticated routing capabilities. Products are available to detect outages automatically by using cross verification among different nodes in a server constellation. If an outage occurs, an event is triggered to modify the traffic flow through either DNS propagation or BGP rerouting. Much like data availability, there is a path to high availability connectivity, but there is a price to pay.

INTEGRATION

As the realities of business change to more of an anywhere, anytime model, the costs of high availability alternatives become more palatable since they create either a competitive advantage or necessity. Well-planned disaster tolerance can be a by-product of the high availability that creates business advantages. That's part of what vendors are selling with the managed off-site data approach. It is also an example of how the process of developing and communicating a Business Continuity Management plan can shape organizational change. In the example in Section I of this article I described our need to mitigate potential losses of $25,000 an hour as the driver that led us to a tighter recovery window and an attempt at a self-healing network. The Business Continuity Management requirement actually drove the ongoing business requirement and provided a competitive advantage as a result.

[3] I assume that your firm sends backup to a remote site once a day and operates 24 hours per day. Murphy's Law will, of course, increase the time since last backup to 24 hours or more.

Table 1. Cost-Risk Tradeoff

Traditional Information protection strategies - Back up Storage Devices - Offsite storage of tapes	**In – house high availability: On-site replication** - RAID, Mirroring, shadowing, shared storage, co-located or redundant servers	**Managed high availability: Off-site data availability + disaster tolerance** - Multi-level remote mirroring with offsite data and system accessibility
Challenges - Time and difficulty of retrieving and restoring data - Manual intervention - Restore process sometimes unreliable	**Challenges** - Time and cost of restoration to clustered environment - Provides no catastrophic disaster recovery capabilities - Pressure to maintain dedicated nature of redundant capacity - COST	**Challenges** - Service offering is complex and requires high speed backbones (can create a different point of failure) - New technologies have reduced cost, but still not viable for all systems - COST
Benefits - Lowest cost - Good solution for non-time sensitive information	**Benefits** - Improves availability by reducing downtime - Provides a level of protection against data loss	**Benefits** - Shortens recovery window - Near zero data loss - Minimal tape backup and offsite shipment - Provides disaster tolerance - Provides expertise at time of disaster

VI. LESSONS LEARNED FROM SEPTEMBER 11

We can only hope that there will never again be as significant a Business Continuity Management challenge as the one that took place on September 11, 2001. The human loss was obviously horrific. Even from a strictly business viewpoint, the scope of the event was beyond the imagination of most plans. Take for example the geographic separation of data centers. Some affected companies had hot sites a few blocks from the World Trade Center. They envisioned a fire or flood in the building and anticipated that moving quickly to a site close by would be optimum. No one thought that blocks of buildings would be closed. Other companies, which planned to reestablish computing activities at any of several hot site locations around the country, avoided that problem. However, when all air travel was suspended so were the plans that included overnight movement of people, tapes, and hardware. But companies did get back in business, many in hours most in days. Following are some of the lessons learned:

- *Have a Business Continuity Plan*. Communicate it, rehearse it, keep it updated. Surprisingly a recent CIO Insight Poll of 258 CIO, CTOs & IT VPs (Bolles and Kirkpatrick, 2001) reported 21% did not have a disaster recovery or contingency plan. Several companies cited recent testing and planning for Y2K as something that really helped prepare for the event.
- *Well-designed plans really work*. Some companies with a large presence in the World Trade Center were back in business in hours (American Express, Merrill Lynch). NASDAQ resumed business in 6 days.
- *Investment in continuous availability strategies paid off*. Critical systems with real-time fail-over capabilities kept the flow of information and the ability to serve clients going both immediately after the crisis and in the weeks that followed.

- *Decision making and communication channels were stretched to the limits*. Telephone and other communications systems were overloaded or destroyed. Critical messaging systems and email were slowed.
- *Companies with clearly defined crisis strategies were able to mobilize their employees and keep major business functions running*.
- *Outsourcing vendors that did not contractually guarantee specific continuity requirements sometimes terminated services*. Business Continuity Management is often missed as a factor in outsourcing decisions. Nearly every business outsources some IT functions; many do not contract any business continuity requirements.
- *People make the difference and planning for the impact on the people was generally the biggest deficiency*. Remember this is Business Continuity Management not Technology Continuity Management. It is about getting the business running, not necessarily the systems. Few plans understood the psychological toll this kind of event would extract. At least be sure the basic creature comforts are attended to and recognize that stress and psychological relief must be included. Cross-train personnel in alternate facilities for business recovery operations and plan and test your ability to engage and move staff. Try to get back to "normal" as soon as possible for both working conditions and business activities.

VII. FINAL THOUGHTS

The world we live in is changing every day and the threats to business continue to multiply. As our systems become more sophisticated and business becomes more reliant on Information Technology, adequate Business Continuity Management is a basic requirement not a luxury. The cost of failure to plan, test and invest is just too high. The days in which we could hope to run most businesses without computers are gone. The days in which our in-house computers could run our business without interface to the outside world are gone. Businesses that hope to be able to sustain success must make the necessary investment in Business Continuity Management.

By the way, since I started writing this article, we've shrunk our recovery window to 24 hours. Moving back up the continuum!

Editor's Note: This article was received on May 2, 2002 and was published on June 12, 2002.

REFERENCES

Bolles, G and Kirkpatrick, T (2001) "Disaster Recovery," CIO Insight, http://www.cioinsight.com/article/0,3658,apn=2&s=304&a=19552&ap=1,00.asp (October 1, 2001)

ABOUT THE AUTHOR

Jeff Hecht is Vice President of Information Technology for Word and Brown, a privately held California corporation in the health insurance industry. Over the last 20 years he held positions in information technology management, including Vice President and Chief Information Officer, with several companies in the financial services sector.

Communications of the Association for Information Systems

ISSN: 1529-3181