Business Continuity Management:

Developing a Process, Not Just a Plan

Jeremy W. Reynolds

February 20, 2004
GIAC Security Essentials Certification (GSEC)
Version 1.4b, Option 1

Abstract

Business continuity is a dynamic process that has changed dramatically over the past ten years, moving from simple disaster recovery plans that focus only on information technology and system recovery to overall plans that include all aspects of the business, from IT to Human Resources. In the modern world, business continuity has become a management process that is constantly reviewed, updated and tested so that it accurately reflects the business environment.

So what is Business Continuity Management and how has it changed in the recent past? Why should a company create plans for business interruption? This paper will answer those questions and discuss key industry drivers that are forcing companies to take a more proactive approach to business continuity. In addition, two methodologies for creating a business continuity management process will be presented along with several approaches that corporations can utilize to implement those methodologies.

Introduction

An inevitable trend developed in the late part of the 20th century; businesses, both small and large, became increasingly dependent on information systems. Advancements in computer and networking technologies, along with rapid expansion of the Internet and seemingly endless economic growth, afforded companies in various industries the ability to improve their market share and expand their businesses into markets that were previously impenetrable. "The widespread use of information systems and the Web has changed the way we do business to a point at which business, the government and our national infrastructure rely on information systems."[1]

As the year 2000 approached, bringing with it the dreaded "Y2K bug" that the public feared would crash all computer systems, executive management looked towards their security leaders for assistance. Disaster recovery plans, which focus mainly on system continuity during disasters, quickly became the focal point of many management meetings, where large percentages of corporate budgets were suddenly allocated for their creation. The prospect of conducting business without the availability of critical systems was too much to endure for many CEOs.

Building upon that, after the tragic events of September 11, 2001, a realization swept through corporations and small businesses around the world. Not only could a disaster disable critical business systems, it could also eradicate vital assets (e.g., people, facilities, customer and company data, etc.) that are critical to the continued existence of the business. With this understanding came a shift of focus from information systems recovery to a more comprehensive overall business continuity management approach.

Business Continuity Management

According to the Disaster Recovery Institute International (DRII), a recognized certification and education leader in the industry, business continuity planning is "the process of developing advance arrangements and procedures that enable an organization to respond to an event in such a manner that critical business functions continue with planned levels of interruption or essential change."[2]

While developing a good continuity plan is essential to a business for maintaining desired service levels, creating a process to test and update that plan is equally critical. It is hard to determine which scenario is worse: having an inadequate continuity plan which does not reflect the current business environment or having no plan at all.

Therefore, a process should be created that not only defines responsibility for developing a business continuity plan, but also one that establishes a

[1] Price, http://www.simon-net.com/st-and-d/articles/article_archives.asp?action=details&magarticle_id=1092
[2] DRII, http://www.drii.org/associations/1311/files/glossary.pdf

comprehensive business continuity management process, one that focuses on the people and processes surrounding the plan, not just on the disaster recovery/ information systems recovery aspects. This type of process can be referred to as Business Continuity Management, or BCM. From this perspective, BCM is more than just a plan:

> Business Continuity Management is a holistic management process that identifies potential impacts that threaten an organisation and provides a framework for building resilience and the capability for an effective response which safeguards the interests of its key stakeholders, reputation, brand and value creating activities.[3]

Three major components that make up the BCM process are:

- Crisis Management: A series of actions taken to gain control of an event quickly to minimize the effects of an interruption, preventing further personnel injury and facility/equipment damage. Crisis communications, which refers to managing all communications during a crisis, both to internal employees and external third parties, is a subcomponent of crisis management.
- Business Resumption Planning: Procedures initiated to resume business operations to a level consistent with the requirements outlined by the business management.
- IT Disaster Recovery Planning: The recovery of information technology systems, applications, databases, and network assets used to support critical business processes.

As stated above, BCM should be an overall approach that focuses on people and processes in addition to information systems recovery. It should include testing and documenting procedures, developing a crisis organizational structure, creating an emergency operations center (from which resumption plans can be coordinated), determining alternate processing facilities, training personnel, creating procedures for communications during a crisis, identifying vital records and customer information, establishing a maintenance program, etc.

How has BCM Changed?

Several key events in the past have had a dramatic impact on the way all businesses conduct their daily operations. One event stands out from the rest.

Following the tragic events of September 11, 2001, corporations worldwide began to realize that a simple disaster recovery plan was not sufficient to ensure business continuity. After all, what disaster recovery plan accounted for the possibility of total facility, equipment, and/or personnel loss?

[3] BCI, http://www.thebci.org/GPGMain.html

Additionally, many business continuity planners failed to look outside of regional risk factors and "worst-case" scenarios when developing plans. After the attacks on the World Trade Center and the total destruction of the infrastructure surrounding the area, it became apparent that continuity planners must expand outside of normal disaster scenarios when determining the risk landscape that their companies must confront. "For many, 9/11 has skewed risk perception in America to the point where some will place terrorism higher than fire and natural disasters common to their region."[4]

The following matrix describes how various aspects of Business Continuity Management have changed since September 11, 2001:

Before 9/11	**After 9/11**
Perception that acts of nature represent the most likely sources of large-scale physical disaster.	Intentional, targeted acts of terrorism carry a high degree of loss potential for organizations, and may be more probable if a particular company has a high vulnerability as a terrorist target (e.g., a company in the World Trade Center).
Business recovery plans tend to assume no limited or temporary loss of key personnel.	Because of the sudden and lethal nature of disasters, key personnel may become long-term or permanent casualties unable to assist in recovery operations. Personnel depth charts and cross-training must be extensive.
The range of threat scenarios focuses primarily on adverse events directly involving/impacting the physical company (e.g., flood, loss of IT resources, etc.).	Indirect threats impacting a company's operations have increased in likelihood (e.g., loss of key customers/vendors, damage to critical infrastructure, including communications, transportation, etc.).
Business continuity plans frequently were limited to IT disaster recovery plans.	Organizations must realize that the ultimate goal of business continuity management is the recovery of critical business processes as well as critical systems that support these processes.
Little consideration was given to "human factors" in the development, testing, training, and maintenance of business continuity plans.	Efforts addressing human factors (e.g., crisis counseling, personnel safety, communication centers, assistance in family contingency scenarios, etc.) are critical elements in ensuring the physical and mental well being of employees, and providing for rapid recovery of business operations.

[4] Holton, http://www.protiviti.com/knowledge/current_feature/021304.html

Before 9/11	**After 9/11**
Business interruptions were viewed as events of relatively short duration, with minimal site displacement requirements and the assumption that data stored "on-site" were accessible.	Realization that business disruptions have an increased potential of long term duration and extensive "off-site" displacement requirements.
Chaos and confusion tended to be underestimated, with limited attention to development of emergency response teams, facilities, and procedures.	Disasters tend to compound chaos and confusion, increasing the necessity for clear, concise, and simple emergency response actions to speed up recovery.
Third party "hot site, warm site, and cold site" vendors utilized tend to be in the same geographic location as the company, and provide "first come, first serve" services to their clients.	Organizations may need to obtain alternate recovery sites that would not be affected by the same regional catastrophe as the primary site. Additionally, organizations must ensure that any third-party vendors are able to meet their contractual obligations to their clients.
Business continuity plans were developed based on a "point in time" philosophy, and did not provide procedures for testing, update, and maintenance.	Organizations need to be proactive at ensuring their business continuity plans reflect the current business environments, including IT infrastructure, business processes, interdependencies and external support.

Although this matrix could be continued for many pages discussing how the attack on the World Trade Center revolutionized BCM, the most relevant topics have been included above.

Other recent events that caught many corporations in the eastern United States by surprise include a large-scale blackout, which left most of the Northeast without power for many hours or days in some cases, and Hurricane Isabelle, which wreaked havoc on transportation and power grids, in addition to loss of life.

Why Should Companies Plan for Business Interruptions?

Now that you have a better idea about what Business Continuity Management is and how it has changed over the past ten years, it is important to focus on key drivers that are virtually forcing companies to create comprehensive plans that are well tested and reflect current business processes.

In addition to the events of 9/11 that have been discussed, other trends have developed that impact continuity. Expectations are higher than ever before, often to the extent that customers demand service 24 hours a day, 365 days a year. Sophisticated computer software and networked systems have created environments that make it virtually impossible for employees to manually complete their job responsibilities. Without these manual "workarounds", the negative impact from any unexpected downtime as a result of a disaster or other interruption has increased exponentially.[5]

Widespread Internet security threats have become increasingly complex in the past ten years also as more and more people acquire access to the World Wide Web. Nearly all companies have connections to the Internet that make them vulnerable to security attacks, such as massive denial of service attacks that render systems unavailable for extended periods of time. Additionally, companies continue to seek ways to increase profits and minimize costs by outsourcing significant IT functions to third party vendors. This is a relatively new trend and, while this strategy can save money, it often results in decentralized IT operations that are difficult to manage.[5] Due to this trend, there is a renewed importance in ensuring that contracts and Service Level Agreements address business continuity issues and recovery requirements.

Another factor that is playing a major role in business continuity management development among corporations in the United States is the increasingly stringent regulatory environment. For nearly every business sector that exists, a corresponding regulation has been developed that requires companies, in some manner, to develop and maintain contingency plans and procedures. Some regulations are listed below:[6]

Federal Government

- Paperwork Reduction Act: Creates security plan for Information Resources requiring contingency planning.
- Computer Security Act: Requires security plans for all federal computer systems to assure data integrity, availability, and confidentiality.
- FEMA FRPG 01-94: All department and agency heads must formally plan for continuity of essential operations.

Financial Services and Banking

- FFIEC FIL-67-97: Board of Directors is responsible for ensuring that a comprehensive business resumption and contingency plan has been implemented, to encompass distributed computing and external service bureaus.
- Comptroller of Currency BC-177: Requires banking institutions to develop and maintain Business Recovery Plans.

[5] Compaq, http:www.intechnology.co.uk/downloads/Compaq/WhitePapers/WHITE_PAPER_E_CONTIN.pdf
[6] Disaster Resource, http://www.disaster-resource.com/articles/00nuggs.shtml

- FFIEC Inter-Agency Policy: Requires business wide resumption planning and extends regulation to require contingency plans from any service bureaus or outsourcing companies which service such banks.
- Gramm-Leach-Bliley Act (GLBA): Requires procedures to protect against destruction, loss, or damage of information from potential environment hazards.

Public Companies

- SEC Regulations: “Reasonable safeguards for information” – These regulations hold the Board of Directors and senior management accountable for business continuity.
- Foreign Corrupt Practices Act (FCPA): Requires that publicly-held corporations provide “reasonable protection for information systems” and holds management accountable.

Medical/Healthcare

- HIPPA: Regulations covering electronic security and transmission of patient records. A documented, tested disaster recovery plan is required.
- Clinical Laboratory Information Act: Requires protection of critical laboratory data.

Other Regulatory Considerations

- NYSE: New Rule 446 (proposed) that includes specific requirements mandating that members develop and maintain written continuity plans, and that they review them on a yearly basis.

The list above is not meant to be a comprehensive collection of all regulations that specifically relate to business continuity, though one can infer with little scrutiny that most companies fall into one of the categories mentioned.

Whether required by law or not, all companies should have implemented, or be in the process of implementing, BCM processes to protect their business and ensure continuous operations in the future should a disaster occur.

Methodologies for Creating a BCM Process

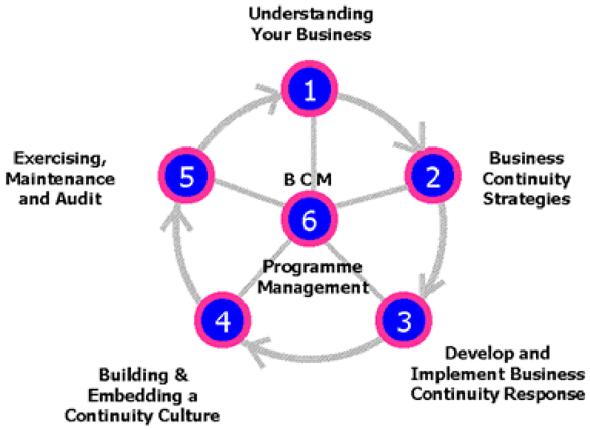
You should now be familiar with Business Continuity Management, how it has recently changed, and key industry drivers that are requiring companies to implement a BCM process.

There are two standard methodologies that are the most widely used when corporations begin a BCM project. First, DRII has developed ten “professional practices” that should act as a guideline when developing a BCM process:

1. Project Initiation and Management: Establish the need for a Business Continuity Management Process or Function, including resilience strategies, recovery objectives, business continuity and crisis management plans and including obtaining management support and organizing and managing the formulation of the function or process either in collaboration with, or as a key component of, an integrated risk management initiative.
2. Risk Evaluation and Control: Determine the events and external surroundings that can adversely affect the organization and its resources (facilities, technologies, etc.) with disruption as well as disaster, the damage such events can cause, and the controls needed to prevent or minimize the effects of potential loss. Provide cost-benefit analysis to justify investment in controls to mitigate risks.
3. Business Impact Analysis: Identify the impacts resulting from disruptions and disaster scenarios that can affect the organization and techniques that can be used to quantify and qualify such impacts. Identify time-critical functions, their recovery priorities, and inter-dependencies so that recovery time objectives can be set.
4. Developing Business Continuity Management Strategies: Determine and guide the selection of possible business operating strategies for continuation of business within the recovery point objective and recovery time objective, while maintaining the organization's critical functions.
5. Emergency Response and Operations: Develop and implement procedures for response and stabilizing the situation following an incident or event, including establishing and managing an Emergency Operations Center to be used as a command center during the emergency.
6. Developing/Implementing Business Continuity and Crisis Management Plans: Design, develop, and implement Business Continuity and Crisis Management Plans that provide continuity within the recovery time and recovery point objectives.
7. Awareness and Training Programs: Prepare a program to create and maintain corporate awareness and enhance the skills required to develop and implement the Business Continuity Management Program or process and its supporting activities.
8. Maintaining and Exercising Plans: Pre-plan and coordinate plan exercises, and evaluate and document plan exercise results. Develop processes to maintain the currency of continuity capabilities and the plan document in accordance with the organization's strategic direction. Verify that the Plan will prove effective by comparison with a suitable standard, and report results in a clear and concise manner.
9. Crisis Communications: Develop, coordinate, evaluate, and exercise plans to communicate with internal stakeholders (employees, corporate management, etc.), external stakeholders (customers, shareholders, vendors, suppliers, etc.) and the media (print, radio, television, Internet, etc.).
10. Coordination with External Agencies: Establish applicable procedures and policies for coordinating continuity and restoration activities with external agencies (local, state, national, emergency responders, defense, etc.) while ensuring compliance with applicable statutes or regulations.[7]

[7] DRII, http://www.drii.org/displaycommon.cfm?an=1&subarticlenbr=7

A second methodology was developed by the Business Continuity Institute (BCI), another recognized industry leader in Europe that is the equivalent of the DRII in the United States. BCI divides the BCM process into six categories and uses the following diagram to illustrate the process:[3]


Understanding Your Business
1
Exercising, Maintenance and Audit
5
BCM
6
2
Business Continuity Strategies
Programme Management
4
3
Building & Embedding a Continuity Culture
Develop and Implement Business Continuity Response

This is a condensed version of DRII's professional practices that consolidates the ten steps into six and presents the methodology as a continuous process. This diagram further illustrates the importance of BCM as a cycle and not simply a plan. There are variations of methodologies that exist, but most resemble one of the two presented here.

Given the above two methodologies, there are many ways a company can go about developing a Business Continuity Plan and creating a management process to keep the plan tested and current. Methods may include using various software products, hiring third party consultants who are experienced in the field and can provide best practice comparisons, and taking the "do-it-yourself" approach, which may or may not include software and/or third party assistance.

Software Products

There are many software packages available to assist companies with developing BCM strategies. One such example is Strohl Systems, a leader in providing complete continuity planning software and services. They provide a suite of complex software applications that assist with various aspects of developing the BCM process, from understanding the various processes within the organization and developing business impact analyses to creating an incident control and emergency operations center from which contingency plans can be initiated and managed.[8]

"Comprehensive planning software provides a wealth of situational information, prompting users to think about scenarios they otherwise overlook. For those with little contingency planning experience, software can help as a guide through the planning process. The tool's automation also saves valuable time and streamlines efforts for a more efficient output."[9] Conversely, software can create

[3] BCI, http://www.thebci.org/GPGMain.html
[8] Strohl Systems Group, http://www.strohlsystems.com/Software/default.asp
[9] CPM, http://www.contingencyplanning.com/Tools/BCPHandbook/purchaseplans/bcpsoftware.asp

a “cookie-cutter” plan that lacks creativity and customization specific to an organization. Small to medium-sized companies (fewer than 200 employees) can often benefit from using software packages since there is relatively little industry knowledge with respect to business continuity within smaller companies and software can provide necessary guidance. It is important to note, however, that some software products can be extremely complex and expensive and should be avoided by very small companies that are seeking a low cost approach.

Additionally, online communities are now available to assist in the creation of a BCM process. For example, Continuity Planner is a member-only forum where you can ask questions from other business continuity professionals and look up industry best practices. They also provide a repository for research and document templates so planners do not have to spend countless hours searching the Internet for valuable information.[10] These types of resources can be a vital asset to small companies looking for an easy approach to creating and maintaining a business continuity management process. However, like software products, these solutions sometimes fall into the “cookie-cutter” category and lack the flexibility that is often required.

Consultants

Another approach to developing a BCM strategy is to hire an outside consulting group or third party contractor. Consultants are highly skilled when it comes to industry best practices since their job is to assist other companies with implementing similar projects. A major advantage with this method is that it is a “one-stop shop”. For an agreed-upon price, consultants, such as KPMG and Protiviti, can create a BCM process from beginning to end and train personnel to maintain and update the contingency plans on a regular basis. With this approach, management can get a complete idea of what the project will cost, how long it will take, and what can be expected when the project is complete before committing resources and funding the effort. Additionally, consultants can avoid the potential pitfalls that may be caused by using software packages because consultants can customize a BCM process specific to your organization.

One key disadvantage of this approach is that companies must share vital information about their operations when they hire an outside party to implement a BCM process. There are inherent risks involved with temporarily hiring a third party into your organization and management must assess those risks and partner with a third party that they trust. In addition, hiring consultants will generally cost more than simply purchasing and implementing software tools since a company will benefit from the skills that consultants bring to the organization.

Another point to consider with using consultants is their ability to transfer knowledge of the BCM process to employees of the organization. After all, once the plan and process is developed, consultants leave the organization and

[10] Continuity Planner, http://www.continuityplanner.com/what_s_in_the_members_area_.html

employees must assume the responsibility of understanding, maintaining, and testing the plan. This type of approach is best suited for medium to large-sized companies (200 to 500 employees), which require customization and flexibility, but also have a larger budget and more resources than smaller companies.

Do-It-Yourself
It can be difficult to determine when and how to begin planning for business continuity. When doing it yourself, any combination of approaches can be utilized to develop a comprehensive BCM process. For example, purchasing a software product to help perform a risk assessment while assigning employees the responsibility of actually creating, testing, and maintaining the plan may be the best solution. This approach generally involves executive management meeting with an assigned continuity planner, who has some experience in contingency planning, from within their organization and determining a project scope. From this point, the planner has the authority to hire consultants or purchase software products as necessary, producing the most customized, cost-effective solution that can be obtained.

The major disadvantage to this approach is the possibility for the project to quickly run over budget, either in time or in cost. The "do-it-yourself" approach is generally best suited for large companies (greater than 500 employees) since these types of organizations have the largest budgets and knowledge pools from which to acquire resources. Additionally, large companies often require deep knowledge specific to internal processes within their organizations that cannot be obtained from purchasing software or hiring consultants.

However, an important note to consider is that, even though very large corporations have many resources, they often still lack the skills to properly implement a BCM strategy without outside assistance. Therefore, a do-it-yourself approach is often the most successful when an organization identifies its own skill sets and utilizes those skills in conjunction with consultants and/or software products as necessary.

Recommendations

After extensive research, I have developed recommendations that will guide an organization to a cost-effective business continuity management solution, regardless of the methodologies and/or approaches chosen. First, and most importantly, executive management should manage the overall process. This is a critical step in successfully implementing a BCM process. As a continuity planner, management "buy-in" to the project is vital so that the importance of the project is not overlooked. Also, since executive management will be held liable if the organization can not withstand a disaster, they should be in charge throughout the project. With executive management leading the way, business continuity coordinators can be assigned at the business levels to carry out the normal continuity operations.

Common standards, policies, and templates should be created to ensure consistency among the business continuity management team. Also, when assessing business risks that an organization faces and evaluating existing controls to mitigate those risks, it is important to utilize internal and external audit reports. These reports often highlight vulnerabilities present in the company that can be overlooked and provide further insight as to the areas that are more critical to the business than others.

Additionally, continuity planners should address business processes and information technology together, as opposed to two separate projects. As discussed in detail throughout this paper, business processes are dependent on information systems in numerous ways. Multiple risk assessments and business impact analyses are costly. If these two areas are analyzed separately, risks can be overlooked and could require additional time and resources. Also, the recovery time objective, which is the agreed-upon amount of time that can elapse after a disaster or other business interruption before a company is severely impacted, must be matched to the most appropriate, cost-effective solution.

Finally, the plan must be maintained and kept up-to-date. A plan that does not reflect current business operations is worthless to an organization. If an appropriate business continuity management process is established, the plan will be current and can be relied upon in the event of a disaster.

Conclusion

It is imperative after September 11th that companies worldwide focus on business continuity and recognize that being unprepared for a disaster could result in permanent negative impact or even total business loss. Given the complexities of many modern businesses, it is no longer appropriate to simply create a business continuity plan and wait for something to happen. It must be a continuous management process, one that is constantly being reviewed, tested, and updated to reflect current business operations.

This paper has defined Business Continuity Management in detail and discussed how the management process evolved from the plan. Detailed information was presented illustrating the changes that occurred in the business continuity industry following 9/11 and other recent events, as well as reasons for creating a comprehensive BCM process. Finally, two methodologies, along with several approaches, for creating a successful BCM process were explored.

Cited References

1. Price, Elaine S. “The Evolution of Business Continuity.” 1 November 2003. URL: http://www.simon-net.com/st-and-d/articles/article_archives.asp?action=details&magarticle_id=1092 (15 February 2004).

2. Disaster Recovery Institute International (DRII). “Business Continuity Glossary.” URL: http://www.drii.org/associations/1311/files/glossary.pdf (13 February 2004).

3. Business Continuity Institute (BCI). “Good Practice in Business Continuity Management.” URL: http://www.thebci.org/GPGMain.html (13 February 2004).

4. Holton, Lisa. “Business Continuity in the Face of a Natural Disaster.” URL: http://www.protiviti.com/knowledge/current_feature/021304.html (15 February 2004).

5. Compaq. “Business Continuity: The new imperative.” 11 June 2001. URL: http://www.intechnology.co.uk/downloads/compaq/WhitePapers/WHITE_PAPER_E_CONTIN.pdf (13 February 2004).

6. Disaster Resource. “Regulatory Checklist.” Planning and Management. 2003. URL: http://www.disaster-resource.com/articles/00nuggs.shtml (13 February 2004).

7. Disaster Recovery Institute International (DRII). “Professional Practices for Business Continuity Professionals.” URL: http://www.drii.org/displaycommon.cfm?an=1&subarticlenbr=7 (13 February 2004).

8. Strohl Systems Group. “Software.” 2003. URL: http://www.strohlsystems.com/Software/default.asp (15 February 2004).

9. Contingency Planning & Management (CPM). “Why Buy?” Business Continuity Planning Software. URL: http://www.contingencyplanning.com/Tools/BCPHandbook/purchaseplans/bcpsoftware.asp (15 February 2004).

10. Continuity Planner. “What’s in the Member’s Area?” URL: http://www.continuityplanner.com/what_s_in_the_members_area_.html (10 February 2004).

Non-Cited References for Additional Research

11. Cowley, Stacy. "Sept. 11 keeps disaster recovery in forefront." 3 September 2002. URL: http://www.computerworld.com/databasetopics/data/story/0,10801,73956,00.html (10 February 2004).

12. Pastore, Michael. "People, Planning Key to 'Business Continuity'." 5 August 2003. URL: http://www.cioupdate.com/trends/article.php/2244581 (13 February 2004).