Preparing a Business Continuity Plan

by James G. Barr

Docid: 00017837

Publication Date: 2006

Report Type: IMPLEMENTATION

Preview

A business continuity plan provides for the continued operation or rapid recovery of a company's critical business functions in the event of a disaster - either natural, such as a fire or flood, or man-made, such as a bombing or computer virus attack. Without a comprehensive business continuity plan, a company may suffer significant losses including revenue, customers, market share, and reputation. In extreme cases, the business may even cease operations permanently.

Report Contents:

- Executive Summary
- Description
- Alternatives
- Challenges
- Step-by-step Implementation
- Web Links

Executive Summary

[return to top of this report]

A business continuity plan provides for the continued operation or rapid recovery of a company's critical business functions in the event of a disaster - either natural, such as a fire or flood, or man-made, such as a bombing or computer virus attack.

Without a comprehensive business continuity plan, a company experiencing a disaster may suffer significant losses including revenue, customers, market share, and reputation. In some cases, a business may even cease operations permanently.

In general, a business function may be considered critical if it:

- Affects a high-profile client.
- Generates significant income or savings.
- Satisfies a legal or regulatory requirement.
- Inspires investor confidence.
- Contributes to the safety and security of the company, including its employees, facilities, customers, and business partners.

The concept of business continuity planning originated in the 1970s as "disaster recovery planning" and was primarily a means of protecting companies against the loss of their mainframe data centers, or "glass houses." In the 1980s, the concept was expanded to include the recovery of non-IT functions and the term "business recovery" was adopted. By the 1990s, with the emergence of e-commerce and other real-time, customer-facing applications, the recovery industry realized that recovery in and of itself was no longer an adequate goal. Especially in the financial services sector, the bar had been raised from recovery to continuous operation. As a consequence, business recovery evolved into business continuity.

Before examining business continuity, which remains the standard for enterprise contingency planning, it's important to explore two rival approaches to business preservation: business resiliency and narrow recovery.

Business Resiliency

The US National Institute of Standards and Technology (NIST) defines resiliency as "the ability to anticipate, withstand, recover from,

and adapt to adverse conditions, stresses, attacks, or compromises on systems." Borrowing on that description, business resiliency, which many business leaders advocate as an alternative to business continuity, provides for the establishment and maintenance of a robust and reliable organizational infrastructure designed to resist any negative consequences resulting from a disaster. Those practicing business resiliency are "all in" on disaster prevention or, failing prevention, disaster mitigation.

Business resiliency is aimed at rendering businesses disaster-proof, thus lowering the odds of actually having to activate a real business continuity plan.

As applied to home office operations, for example, which have become central to many business models as a result of the current coronavirus pandemic, a typical business resiliency plan would likely involve the special provisioning of:

- **Cybersecurity** - Remote security monitoring, patch management, incident response, security awareness training, and other anti-malware software and services.
- **Physical Security** - Safes, home security systems, and anti-theft devices like PC locks.
- **Document Disposal** - The collection and certified on-site destruction of confidential paper documents, computer discs, and USB drives.
- **Telemedicine** - Psychological services intended to counteract the adverse effects of social isolation and other COVID-19-related disorders.
- **Remote Training** - Virtual courses, conferences, and seminars.
- **Social Collaboration** - Software and services designed to facilitate spontaneously creative interactions between employees.
- **Remote Administration** - Software and services intended to facilitate remote workforce management and human resources management.

A Home Office Business Resiliency Plan would be focused on keeping home office operations viable and effective, especially as many businesses will elect to continue, even expand, home office deployments post-pandemic.

Narrow Recovery

Narrow recovery, the author's term, is the selective application of business continuity, and is based, implicitly, on the assumption that most disruptions are ultimately survivable if certain key assets are protected.

For example, a business may choose to safeguard its IT assets (a common occurrence), or its product stores, or essential manufacturing equipment, or key personnel, or some combination of physical and human resources. A business may also choose to consider only certain types of disasters, such as fires, floods, or cyber attacks.

The overall objective is to create a ***lean*** continuity capability which is consistent with the organization's priorities, budget, technical expertise, and management experience. While not ideal, narrow recovery is certainly preferable to no recovery at all.

Description

[return to top of this report]

Business continuity is a process that provides for the ongoing operation or, in the alternative, the rapid recovery of a company's critical business functions and assets in the event of a disaster or major disruption.

Also known as "disaster recovery," "business recovery," and, in government circles, "continuity of operations (COOP)," business continuity poses a conundrum for many executives. While there is general agreement that companies should protect themselves against natural disasters, like hurricanes, or unnatural disasters, like acts of terrorism, there is little or no consensus relative to the big questions:

- **What constitutes a critical business function or asset?** Traditional disaster recovery, for example, is still focused - almost exclusively - on preserving information technology (IT) assets.
- **Which, if any, standards should be followed?** The 9/11 Commission, for example, endorsed the National Fire Protection Association (NFPA) standard on Disaster/Emergency Management and Business Continuity Programs.
- **What level of resources should be applied?** Some companies, for example, budget business continuity as a percentage of their overall IT budget, again reflecting an IT orientation.

In an effort to answer these and other questions, many companies are turning to benchmarking. This is the process of measuring a company's performance - in this case, their business continuity performance - against that of similar companies.

While over the years, several major research firms have conducted business continuity benchmarking studies, these studies are often general in nature and lack the specific apples-to-apples comparisons that would allow one mid-level manufacturing company, for example, to compare its business continuity program against the programs of other mid-level manufacturing firms.

Companies are encouraged, therefore, to conduct their own surveys within their own industry to gauge whether their business continuity program is adequate, and, if inadequate, what initiatives should be pursued to improve their overall business continuity posture.

Performing a business continuity benchmarking survey is fairly straightforward and may be conducted formally (i.e., in writing) or informally (over the phone or via casual conversations). In either case, the goal is:

- To determine what similar companies are doing - or not doing - to affect business continuity.
- To identify - and implement - any best practices as revealed by the survey participants.
- To demonstrate due diligence in business continuity planning.

Identify Survey Subjects

First, identify companies of similar size and business structure, either within your general geographic location or on a wider scale. Contact your business continuity counterpart in each of these companies and open a dialogue relative to benchmarking. If possible, collaborate with several of these individuals to conduct a joint survey. This can save time and money.

Devise Survey Questions

Before initiating a survey, settle on a group of basic questions, like those offered in Table 1.

Table 1. Sample Business Continuity Benchmarking Survey

No.	Questions
1	How much is your company spending on business continuity? How did you arrive at that figure?
2	Do you have a business continuity manager? If not, who has responsibility for business continuity?
3	Is business continuity visible at the C-suite level and/or with the board of directors?
4	Do you subscribe to a particular business continuity standard or guideline? If so, which one?
5	Does your business continuity program encompass non-IT assets? If so, what is the non-IT scope?
6	Does your business continuity program ***converge*** with your security and emergency management programs? If so, how?
7	When do you update your business continuity plans? Are maintenance activities time-based (like every six months) or event-based (as when the business changes)?
8	How often do you exercise your business continuity plan (or plans)? What type of tests or exercises do you conduct? IT-only? Tabletop? Other?
9	Has your company experienced an actual disaster? If so: • What type of disaster? • Did management adhere to the business continuity plan? • Was the business continuity plan generally effective? • Which parts of the plan worked? • Which parts of the plan didn't work?
10	What advice would you offer in developing, documenting, and deploying a business continuity program?

Identify Best Practices

Identify - and implement - any best practices as revealed by the survey. For example, many companies with a large knowledge worker population are implementing "telework" strategies, leveraging their employees' home and mobile computing resources to create ad hoc disaster networks.

Pay particular attention to strategies employed by competitors. In a regional disaster that affects multiple companies, a competitor's ability to expedite recovery could have long-lasting competitive implications, especially if rapid recovery enables client stealing.

Bottom line: Don't let a poor business continuity program become a source of competitive disadvantage.

Alternatives

[return to top of this report]

Not long ago, companies devising business continuity plans were limited to a few variations on a common theme: the recovery site. Options included:

- **Hot Sites** - Fully operational facilities maintained by independent providers who are usually paid a monthly subscriber fee for the availability, space, equipment, and services they offer.
- **Cold Sites** - Computer-ready spaces held in reserve for the client's own systems.
- **Warm Sites** - Data centers or office spaces partially equipped with hardware, communications interfaces, power sources, and environmental conditioning.
- **Mobile Recovery Centers** - Custom-designed structures outfitted with computer and telecommunications equipment and transported to a chosen location.[1]

The recovery site solution was created primarily to allow the recovery of large mainframe data centers. This was - and is - expensive, especially the hot site option, and it rarely satisfies the needs of smaller companies or companies with a decentralized IT infrastructure. The term "rarely" is applied since, today, some providers offer miniature hot site facilities designed to support small-to-medium-sized companies (SMCs).

While the recovery site solution remains a viable business continuity strategy, especially for large companies, a number of less expensive and more flexible strategies have emerged. These include:

- Dual operations centers
- Consolidation and displacement
- Reciprocal recovery
- Telework
- Cloud computing

Importantly, these strategies are not exclusive. One or more may be combined to create a total business continuity solution.

Dual Operations Centers

The theory behind dual operations centers is simple. Instead of creating one operations center, create two. If one center fails, the other remains in operation. Depending on capacity, the surviving center may be able to absorb some - if not most - of the failed center's workload.

The term "operations" is non-specific and is meant to imply a variety of functions. An operations center, for example, may be a traditional data center. However, it may also be a:

- Call, or contact, center
- Manufacturing center
- Product distribution center
- Company administration center

Note: In the data center context, dual operations centers are often employed to provide uninterrupted computer operations, essential for supporting real-time, customer-facing applications. This is typical of financial processing.

Consolidation and Displacement

Consolidation and displacement involve the temporary reallocation or redeployment of company facilities to accommodate displaced workers and functions.

- **Consolidation** "makes use of existing in-company accommodations, such as a training facility or [lunchroom], to provide recovery space or increase ... office density."[2]
- **Displacement** involves "displacing staff performing less urgent business processes with staff performing a higher priority activity. Care must be taken when using this option that backlogs of the less urgent suspended work do not become unmanageable."[3]

Consolidation and displacement share the virtue of not requiring commercial recovery space, although, in actual practice, some "makeover" costs will be incurred, such as installing PCs and other equipment in vacant conference rooms. Also, the consolidation and displacement strategy must be carefully planned. Ad hoc rearrangement of furniture and other facilities could actually complicate recovery.

Reciprocal Recovery

Call it communal recovery. Reciprocal recovery arrangements allow two or more *similar* companies to form a recovery network. Two law firms, for example, could agree to act as each other's recovery site. If one firm suffers a disaster, the other firm would provide emergency relief such as temporary office space, clerical help, etc. In the case of three companies, two could backup one. The larger the network, the larger the pool of recovery resources. Also, the larger the network, the greater the diversity of recovery resources.

Telework

Telework is defined as work performed independent of location. A teleworker is anyone who works from:

- Home (aka, a telecommuter)
- A satellite office
- A client office
- A business partner office
- A telework center

Cheaper than conventional recovery options, telework is not only a viable business continuity strategy but it is gaining in popularity for normal (i.e., non-disaster) operations.

Telework, of course, has become a featured continuity strategy during the current coronavirus pandemic, enabling knowledge workers to operate from home and thus observe government-mandated social distancing restrictions.

Cloud Computing

From popular business software to computing infrastructure to business services, cloud providers like Amazon, Microsoft, Google, and Salesforce provide a wide variety of plug-and-play corporate business functions and resources. With proper planning - and high-speed, secure Internet access - these elements can be arrayed as part of a company's overall business continuity or business recovery solution.

Additionally, when employed on a regular basis, cloud assets can help reduce a company's exposure to business-crippling disasters.

Manual Workarounds

Many automated business processes originated as manual processes. As the US Department of Homeland Security (DHS) reminds us, these automated processes can often be resumed by implementing "manual workarounds."

Identify the steps in the automated process - creating a diagram of the process can help. Consider the following aspects of information and work flow:

- Internal Interfaces (department, person, activity and resource requirements)
- External Interfaces (company, contact person, activity and resource requirements)
- Tasks (in sequential order)
- Manual intervention points

Create data collection forms to capture information and define processes for manual handling of the information collected. Establish control logs to document transactions and track their progress through the manual system.

Manual workarounds require manual labor, so it may be necessary to reassign staff or bring in temporary assistance.[4]

Manufacturing Recovery

Business continuity frequently extends beyond IT recovery to recovery of manufacturing or production facilities. DHS suggests multiple strategies for restoring manufacturing operations:

- Shifting production from one facility to another
- Increasing manufacturing output at operational facilities
- Retooling production from one item to another
- Prioritization of production—by profit margin or customer relationship
- Maintaining higher raw materials or finished goods inventory
- Reallocating existing inventory, repurchase or buyback of inventory
- Limiting orders (e.g., maximum order size or unit quantity)
- Contracting with third parties
- Purchasing business interruption insurance[5]

Challenges

[return to top of this report]

Modern business continuity planning evolved from disaster recovery planning, which began as an effort to protect mainframe computer systems from the effects of fire or other disasters. This IT legacy has both helped and hurt the development of business continuity.

- It helped in raising the profile of business continuity, especially as information systems became more critical to business success.
- It hurt, in many cases, by narrowing the focus of business continuity to data center activities. Even today, most business continuity programs are managed and implemented by IT staff.

Making the most of business continuity investments involves three main issues:

- Managing "real world" disasters
- Protecting non-IT assets
- Conducting adequate plan maintenance

Real World Disasters

Conventional business continuity planning concentrates on worst-case scenarios, such as the destruction of key company facilities. Minor or transient disasters, such as power failures, are all but ignored. Unless the expected duration of the disaster is several days (often a week or more), business continuity plans are not invoked. To achieve relevancy, business continuity planning must be expanded to include real world disasters; in other words, the type of short-term disasters, such as power failures and storm damage, that actually occur.

Non-IT Assets

In addition to dealing with real world disasters, business continuity planning must be enhanced to accommodate non-IT assets, such as vital:

- Paper records
- Manufacturing equipment
- Product inventory
- Distribution facilities

Adequate Plan Maintenance

A business continuity plan is a living document, linked to a company's overall business strategy. As the strategy changes - especially as the company's critical business functions expand, contract, or change in priority - the company's business continuity plan must change to reflect these altered states. Correspondingly, each new generation of a business continuity plan must be thoroughly tested through mock disaster drills.

While some companies use their change management system to trigger a change in their business continuity plan, a more reliable method of ensuring plan currency is to schedule regular maintenance and testing. The standard is at least twice a year, more frequently if practical, and more frequently if the business is undergoing major changes.

No End In Sight

A novel aspect of the current novel coronavirus pandemic is its timeline. Unlike other disasters with predictable durations and outcomes, the Covid-19 infection may linger for years (transitioning from a pandemic to an endemic, or persistent, state). This means that certain continuity actions may become permanent, effectively replacing normal operational protocols and procedures. This eventually should be addressed in the business continuity plan, perhaps by incorporating a business reengineering phase in which business processes are gradually renewed and improved as business conditions evolve.

Step-by-step Implementation

[return to top of this report]

While no two business continuity plans are the same, the process of preparing a business continuity plan is fundamentally similar from company to company. There are seven basic steps to implementing a business continuity plan, incorporating four distinct phases. These phases, as illustrated in Figure 1, are Business Impact Analysis, Recovery Strategies, Plan Development, and Testing & Exercises.

Figure 1. Business Continuity Planning Phases

Source: Ready.gov | US Department of Homeland Security[6]

Step 1: Create a Business Continuity Planning Team

Companies need to remember that, while most business continuity programs originate in a company's IT department, business continuity is a whole-business effort and not just an IT-based initiative. To ensure that all critical business functions are addressed, the business continuity planning team must consist of representatives from all major corporate functions, including finance, legal, sales and marketing, manufacturing, production and distribution, and human resources. Issues of regulatory compliance and security are making it increasingly important to involve all stakeholders in the decision.

Step 2: Conduct a Business Impact Analysis (BIA)

A business impact analysis (BIA) is a form of risk analysis performed by business continuity professionals.

A BIA should be carefully calibrated to achieve the following:

- The identification - and prioritization - of critical business functions.
- A determination of the recovery time objective (RTO) of each critical business function. RTO is a measure of how long a function can be unavailable without significant harm to the company.
- A list of likely disaster scenarios and the impact of each scenario on each critical business function. For example, in a retail setting, the loss of Internet access may have little impact on store operations. It would, of course, have a crippling impact on e-commerce operations.

One "back door" method of conducting a business impact analysis is to identify which business functions would be seriously effected in the absence of key resources. Completing Table 2 is a good place to start.

Table 2. Identifying Critical Business Functions Based on Key Resource Loss

Key Resource Loss	Precipitating Event	Effected Business Functions	Critical/ Non-Critical)
Essential Personnel, including senior management and technical staff	• Retirement • Resignation • Termination • Prolonged Illness or Injury • Internal Transfer • Kidnapping (especially foreign travelers) • Imprisonment (especially foreign travelers) • Death (natural, accidental, or as the consequence of an active shooter or other workplace incident)		

Vital Facilities, due to physical damage or loss of access	• Tornado • Hurricane • Earthquake • Fire • Flood • Explosion • Bombing • Sabotage • Civil Disruption • Loss of Municipal Utilities (Gas, Water, Electric)		
Principal Business Partners	• Business Partner Bankruptcy • Business Partner Disaster • Failure of Business Partner's Business Partners (second-level supply chain breaks)		
Major Information Systems	• Hardware/Software Failure • Cyber Attack • Insider Attack • Internet/CDN Outage		

Step 3: Devise Continuity/Recovery Strategies/Processes

Here's the hard part. Business continuity planners must devise a continuity/recovery strategy or process for each critical business function. A continuity strategy or process implies uninterrupted operations; a recovery strategy or process implies a short period of downtime followed by the resumption of normal - or near normal - operations. A continuity/recovery *strategy* specifies a general approach to continuity/recovery. A continuity/recovery *process* prescribes a precise set of procedures for achieving continuity/recovery.

Step 4: Appoint a Business Continuity Operations Team

In the event of a disaster or other major disruption, continuity/recovery operations will be conducted by a Business Continuity Operations team. Ideally, team members should have crisis or emergency management experience, be committed to the concept of business continuity, and be empowered to make tough decisions in what may evolve into a chaotic environment.

Step 5: Develop a Business Continuity Plan Document (BCP)

Business continuity operations should be codified in the form of a Business Continuity Plan document. The document should state under what circumstances the plan will be activated and detail the various continuity and recovery strategies and processes. A vital part of the plan is contact information, ensuring that all employees and supply chain partners are accessible, especially during off hours.

Step 6: Conduct an Initial Business Continuity Test

No plan can - or should - be considered viable without a comprehensive test. Since test events tend to be disruptive, the testing process can be divided over several small-scale exercises.

Utilize tabletop exercises to allow business continuity team members to experience disaster management in a "no-harm, no-foul" environment. A tabletop exercise is conducted in the manner of an improvisational drama, complete with "twists and turns" and no prescribed or even predictable ending. Typically, an exercise is performed from a script in which major plot points are revealed but the actors (the team members) are responsible for filling in the scenes. A good tabletop exercise might feature the mock destruction of company headquarters. Positioned around a conference table (hence the designation "tabletop"), team members would invoke their portion of the overall business continuity plan, interacting with each other as necessary and expedient. The exercise moderator, probably a third-party crisis manager, would introduce unexpected elements to the exercise, like a regional power failure, to determine:

- Whether the business continuity plan is sufficiently robust to deal with dynamic events.

- Whether the business continuity team members can meet the challenge of managing an event that does not proceed "by the numbers."

Step 7: Educate Employees and Other Continuity Stakeholders

Finally, employees and other stakeholders should be introduced to the Business Continuity Plan, and informed what their responsibilities will be in the event - however unlikely - that the plan is activated.

Web Links

[return to top of this report]

Business Continuity Institute: http://www.thebci.org/
Continuity Central: http://www.continuitycentral.com/
Continuity Insights: http://www.continuityinsights.com/

References

[1] "2003 Master Source Buyer's Guide." *Contingency Planning & Management*. 2003.
[2] "Business Continuity Management Good Practices Guidelines (2005)." Business Continuity Institute. 2005.
[3] *Ibid*.
[4] "Business Continuity Plan." US Department of Homeland Security.
[5] *Ibid*.
[6] *Ibid*.

About the Author

[return to top of this report]

James G. Barr is a leading business continuity analyst and business writer with more than 30 years' IT experience. A member of "Who's Who in Finance and Industry," Mr. Barr has designed, developed, and deployed business continuity plans for a number of Fortune 500 firms. He is the author of several books, including *How to Succeed in Business BY Really Trying*, a member of Faulkner's Advisory Panel, and a senior editor for Faulkner's *Security Management Practices*. Mr. Barr can be reached via email at jgbarr@faulkner.com.

[return to top of this report]