

What is “Business Continuity”? And Why Do I Need It?



What happens if... the key question to planning for sustaining your business when the unexpected happens.

What happens if your business area is hit by an earthquake? Earthquakes, tornadoes, and hurricanes are the types of events that we typically associate with a need for “Business Continuity”. Since the events surrounding September 11, 2001, businesses are well aware of the threat of terrorism and sabotage, but what about common occurrences such as power grid failure, the discovery of asbestos or carcinogens in the workplace, or the impact of computer viruses, corrupted data, or equipment failure? Will your company be able to remain in business without having access to your business data for extended periods of time?

These are the first of many questions that start with “what if...” and if the answer to any one of them is “my business might fail,” then you cannot afford to ignore the benefits of a Business Continuity Plan.

Probably one of the most frustrating areas for business owners, managers, and entrepreneurs is dealing with all those unplanned, unanticipated things that always seem to happen to a business at the worst possible time. Whether it’s a tragic emergency or just the extended vacation of a key employee, these events distract from the main line of business. And, as every business owner knows, these events can destroy a business overnight if there are not sufficient strategies and procedures in place to deal with them. No matter how large or small the event – or the business – if your business cannot sustain the shock, it will fail and disappear. It may not disappear quickly; it can take years to resolve all the issues and liabilities of a failed business, making the demise of a business much more painful than the start-up.

This is the area of risk analysis and contingency preparation known as **Business Continuity Planning**. It covers a wide range of events from significant catastrophes to the more mundane distracters that, if left to themselves, will cripple or perhaps entirely wipe out your bottom line.

Unfortunately, because these events are outside the normal line of business, most companies typically don't plan or prepare until one happens. By then it may be too late.

Here's what you can do for your business to protect it.

1. Identify Critical and Key Business Processes (what do you *have* to do every day, every week to stay in business).
2. Conduct an impact analysis (what are the possible risks to those business processes and what is the cost impact on the business).
3. Quantify risk (what is the likelihood a particular risk will emerge).
4. Implement processes and safeguards to minimize risks.
5. Define procedures to implement in the event a risk materializes.
6. Test the plan, procedures and processes.

The categories of events you should consider when identifying risks should include:

Catastrophic Events: Floods, fires, tornadoes, explosions involving company property or assets.

Medical Emergencies: Accidents, sudden illness, or sudden death of company personnel or visitors to company property.

Loss of Key Personnel or System: Database crashes, long-term illnesses, vacations, people who quit, or people who must be fired.

Unplanned Closures: Office or plant closures due to weather, power outages, or neighboring emergencies (if the office next door burns down, you may have to close for a day or longer).

Planned Closures: Office remodeling, street repairs, computer system upgrades.

Business Shock: Loss of key supplier, large customer, an unanticipated debt recall, an adverse litigation result.

Market Shock: Large, fast shifts in the market or the economy.

During an actual emergency, implementation of the appropriate business continuity plan will generally follow these steps:

- 1. Contain the event.** For example, say one of your employees has a heart attack at the office during the workday. Obviously, the first thing to do is to get them to the nearest hospital.
- 2. Operate critical systems.** Critical systems are those that absolutely must be available under the conditions of the emergency. In our example, your company's communications system is critical – from calling 911 (who dials?) to notifying management and Human Resources (who calls next of kin?), this system must run smoothly and quickly. Other systems may be critical as well, depending on the business. Say this employee was a pet groomer, then you'll want to ensure the pets they were responsible for are safe and in their cages. If the employee was a production line worker curing materials in an oven, you'll need to ensure production continues, if only to take the material out of the oven to prevent a subsequent emergency (who checks to make sure the area is safe?).
- 3. Resolve the event.** Resolution in our example continues long after the employee is taken to the hospital. There will be forms and paperwork, concerned coworkers and a period of stress in the workplace.
- 4. Operate key systems.** Using our pet groomer example, someone will need to return the pets to their owners (will they be groomed?) and call the next days appointments (cancel, reschedule, or bump to another groomer?).

5. **Conduct recovery.** This is restoring your business processes. If the employee in our example was a customer relationship manager rather than a pet groomer, then someone will need to get into the employee's computer to get contact information and ensure the customers are serviced (anyone have the password? Is the employee using standard data and software so you can find the information?)
6. **Return to normal business.** Perhaps our story will end well and the employee will return to work shortly. Then again, maybe their recovery will be long and you'll need to hire a temporary. Or they may never return at all and you'll need to hire a new person. Do you have the systems in place to transfer the key employee's knowledge to your new employee? How long until you can bring that new person on board, how long until they are fully productive?
7. **Review Lessons Learned.** Be sure to conduct a Lessons Learned Review after any significant event and check how well the plan worked. Gather the people who were affected by the event, as well as those who were responsible for recovery activities. Ask them what processes or procedures failed, need improvement, or were unnecessary? What worked well? What in the plan should be changed, added, or deleted? Learning from experience is one of the most valuable tools for preventing or mitigating worse disasters in the future, but it only works if the experience is captured and applied.

A good business continuity plan will go a long way to making your decisions clearer and easier under unusually stressful conditions. Our example above was a relatively simple incident. Imagine if a virus suddenly erased the hard drives on your computer one morning. Do you have backup data to restore your system? How long can your people perform meaningful work without their computers before they become idle? Do you need backup systems that are ready to go, or is it cheaper to simply buy a new system if and when such an event should happen? Much depends on the nature of your business.

There are, however, certain safeguards every business should have in place.

1. Ensure you have appropriate levels of property, liability, and medical insurance.
2. Implement procedures that require employees to document and safeguard key elements of business information in a standard and secure fashion.

3. Conduct routine backups of critical database systems (two backups, one located with the database for quick recovery, one offsite for physical protection.) Paper files are not a good solution; if you have critical paper files, you have a significant backup and offsite storage issue. Just ask the thousands of military veterans that have lost benefits because of the fire at the National Records Retention Site 40 years ago.
4. Consider having backup systems at an alternate location. This may be a full suite of computers in a standby office space (Companies with more than one office usually pair offices into complementary backup sites), or it may simply be a laptop at home.
5. Establish succession plans. Ensure everyone knows who is in charge if you are not there. Ensure your successors have access to the information they'll need to make decisions on your behalf.
6. Establish and test notification rosters. Create a phone tree by which you can alert all your employees at home should there be an emergency. Don't expect one person to call all your employees, and don't keep your phone list only at the office.
7. Establish evacuation plans and conduct rehearsals. You should do this whether you have an established office or a home-based business. Ensure everyone knows how to get out of the building safely, and where to rally once outside.
8. Maintain a business plan that accounts for an appropriate level of financial shock. Know what the potential cost is of an emergency or unplanned event to your business. Maintain an appropriate cash reserve or establish an available line of credit that you can tap quickly. If you have a sound plan, you'll know what level of disaster business can survive, and at what point you may have to call it quits. Have a plan to liquidate your business. If you receive a shock you know your business can't survive, having a sound exit strategy will ensure you don't go deeper into debt or be burdened by preventable litigation.

Business Continuity Planning can be complex and difficult. However, the risks of not having a sound plan are exceedingly high. We, at Vega & Associates, Ltd., have developed or participated in the development of many Business Continuity plans over the years, and we have witnessed quite a few disasters and led many successful recoveries as well. Let our expertise help you develop a viable and workable Business Continuity Plan. The result will be

faster, more complete, and at less cost than it would probably take you to develop one on your own.

...What if an emergency occurs?

You'll be prepared!

This WhitePaper was prepared by Vega & Associates, Ltd., a technology consulting firm that is expert in the design and deployment of strategic, value-driven technology solutions. Visit us at www.vnaltd.com, or call us at 817.379.9952.